

IBM Digital Asset Haven

Your unified platform to custody, transact, govern, and settle digital assets across multiple blockchains.



IBM

Home

Funds

Transfers

Wallets

Organisation

Users

Policies

Keys

Settings

Home > Wallets

Wallets

Q Search...

Filter

Create a Wallet

Name	Balance	Address	Created at
USDC Treasury Wallet	1.800.140,00	0x029uamq874kf99...	Jun 13, 2025 1:39 pm
USD Account	720.000,00	0x023rwkg034kfef...	Mar 11, 2025 7:47 am
EURC Account	320.700,00	0x023rwkg034kfef...	Jul 11, 2025 7:47 am
Pound Wallet	100.200,00	0xa13rwup1uik123...	Jul 29, 2025 8:57 am
Euro Wallet	80.200,00	0xa13rwup1uik123...	Jul 29, 2025 8:57 am

Users

Manage your users.

Q Search...

Filter

Operator

Employee

CustomRole

+ add a user

Permission name

Allowe

Admin

All

Operator

Sign

Employee

Billing,

CustomRole

Custom

4 of 4

Digital Asset Market Trend

Trillions in assets, payments, and market systems are moving to programmable rails.

Key market trends

\$18.9 Trillion in Tokenized Assets by 2033 (Boston Consulting Group)
Securities, commodities, real estate, and cash equivalents are becoming tokens on the chain.

CBDCs in Over 100 Countries
More than 20 in pilot or production, including China (e-CNY), Brazil (DREX), ECB (Digital Euro).

Stablecoins Are Mainstream
The annual stablecoin transfer volume reached \$27.6 trillion in 2024, surpassing the combined volumes of Visa and Mastercard by 7.7% (McKinsey, WEF).

Institutional Adoption Accelerating
Global tier-1 institutions run pilots and MVP’s for custody, tokenization, and institutional lending.

Why it matters

New Revenue Pools
Custody, settlement, payments, and capital markets infrastructure are migrating to blockchains.

Operational Efficiency
24/7 markets, instant settlement, programmable compliance, and lower costs enable more capital efficiency and new business models.

Market Imperative
Banks, payment services, and governments review offering digital asset services to address being challenged by fintechs and blockchain-native challengers.

IBM Infrastructure Advantage
IBM already today provides the foundational infrastructure, securing and scaling transaction processing.

2024



Challenges: Foundational and beyond

Regulatory Compliance

Most players in the digital asset market have yet to proof full regulatory compliance & that their solutions enable receiving license approvals to operate globally.

Cross-Business Complexity

Rolling out digital assets across payments, banking, card issuing, and other units adds significant coordination challenges and integration friction.

Long-term Partnerships

Institutions seek long-term, trusted technology partners to support and enable their digital asset journey.

Fragmented Operational Stacks

The market is constrained by siloed systems for accounts, permissions, transactions, compliance, custody, and issuance create costly inefficiencies and limit scalability.

Institutional-grade security

The digital asset market lacks long-term track records of providing truly bulletproof security — a standard that traditional financial institutions have built & proven over decades.

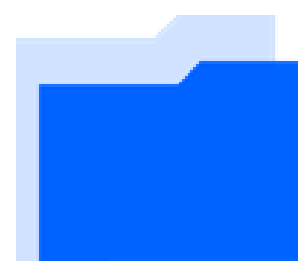
Enterprise Workflow Misalignment

Blockchain infrastructures often fail to integrate with institutional approval chains, compliance protocols, and enterprise systems, stalling adoption.

Meeting these challenges requires a unified, scalable, and secure digital asset platform.

IBM Digital Asset Haven

IBM Platform



Wallets as-a-Service (Waas)

Create and embed digital asset wallets into their systems. These wallets can trade on multiple blockchains, automate address creation for easy deposits, send real-time transfer notifications, track balances, and move funds efficiently through compliance checks and liquidity providers.



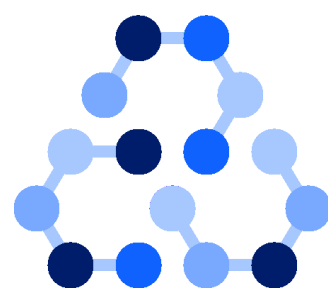
Transaction Management System (TMS)

Orchestrate onchain transfers with full policy control, KYC integration, and real-time monitoring. IBM's Transaction Management System provides a secure, auditable system to orchestrate, approve, and track every onchain operation through a single API.



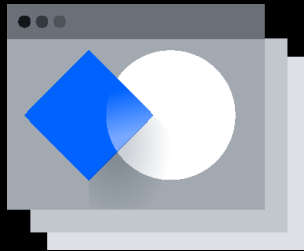
Wallet Entitlement Management (WEM)

Create and manage user roles, permissions, access controls, transaction policies and last-mile validations across all chains. WEM offers granular governance over who can initiate, approve, or view transactions, and create new transaction policies, ensuring compliance and security over digital asset operations.



Key Management Service (KDS)

Orchestrate keys across multiple environments from a unified interface. IBM provides MPC key management as well as a BYOD API, allowing enterprises to connect their IBM Z® & IBM® LinuxONE Hardware Security Modules (HSMs) and IBM Trusted Execution Environments (HPVS).



Integrations



Wallet as a Service (Waas)

Wallet APIs
Automate multichain wallet creation inside your workflows and operations.

Embeddable Wallets
Seamlessly integrate fully capable wallets into apps to onboard users instantly.

Passkey Wallets
Secure wallet access with biometrics, PIN, passwords, U2F devices, and more.

Multichain Wallets
Interact with all blockchains networks with full indexing of all token standards.

Tags & Automations
Automate transactions between any wallet (e.g., deposit ↔ treasury wallets).

Webhooks Alerts
Detect incoming and outgoing transfers, notify users, create triggers, and automate.

Flexible Configurations
Create either company- or user-controlled wallet for security or regulatory reasons.

Transaction Management System (TMS)

Transaction Formatting
Create transaction payloads for any token including fees, memos, travel-rule data, etc.

Transaction Broadcasting
Broadcast any transaction, including contract calls, with full lifecycle tracking.

Transaction Automations
Automate transfers with webhooks and triggers for recurring or conditional flows.

Transaction Routing
Automate flows by selecting optimal routes for transfers, swaps, and buy/sell options.

Transaction Delivery
Avoid failed transactions with automatic queuing, retries, and full stack redundancy.

Transaction Compliance
Add checks into policies, blocking/freezing abnormal activity while enforcing AML/KYT.

Wallet Entitlement Management (WEM)

Programmable Governance
Automate transaction approvals with APIs embedding governance logic into apps.

Identity & Access Management
Assign dynamic roles and granular permissions for wallets, users, and actions.

Transaction Policies
Set rules by user, time, size, frequency, external data and other variables.

Admin Quorums
Require group consensus before sensitive actions, preventing unauthorized execution.

White- & Blacklisting
Restrict flows with approved addresses and block known malicious actors.

Full Data Integrity
Ensure accountability via passkey-based signing and tamper-proof audit trails.

Key Management Service (KDS)

Bring-Your-Own-Device API
Connect IBM LinuxONE & IBM Z HSMs to our SaaS APIs & manage keys on-prem.

Distributed MPC Signers
Distribute MPC keys across environments, eliminating single points of failure.

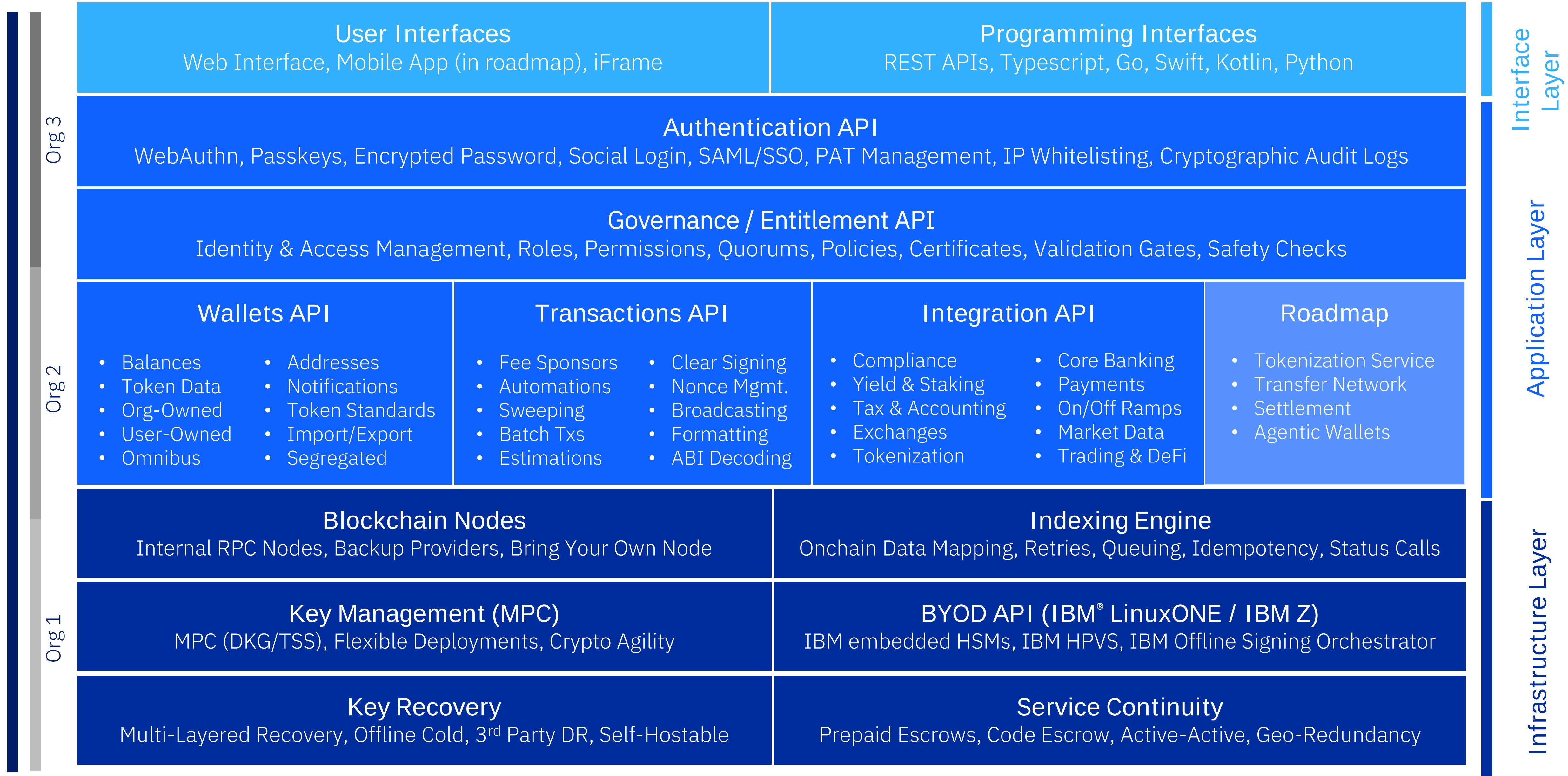
Flexible Signing Thresholds
Set quorum-based policies with thresholds to reduce risks from rogue insiders.

Configurable Recovery
Deploy backup keys globally, ensuring recovery under outages or legal restrictions.

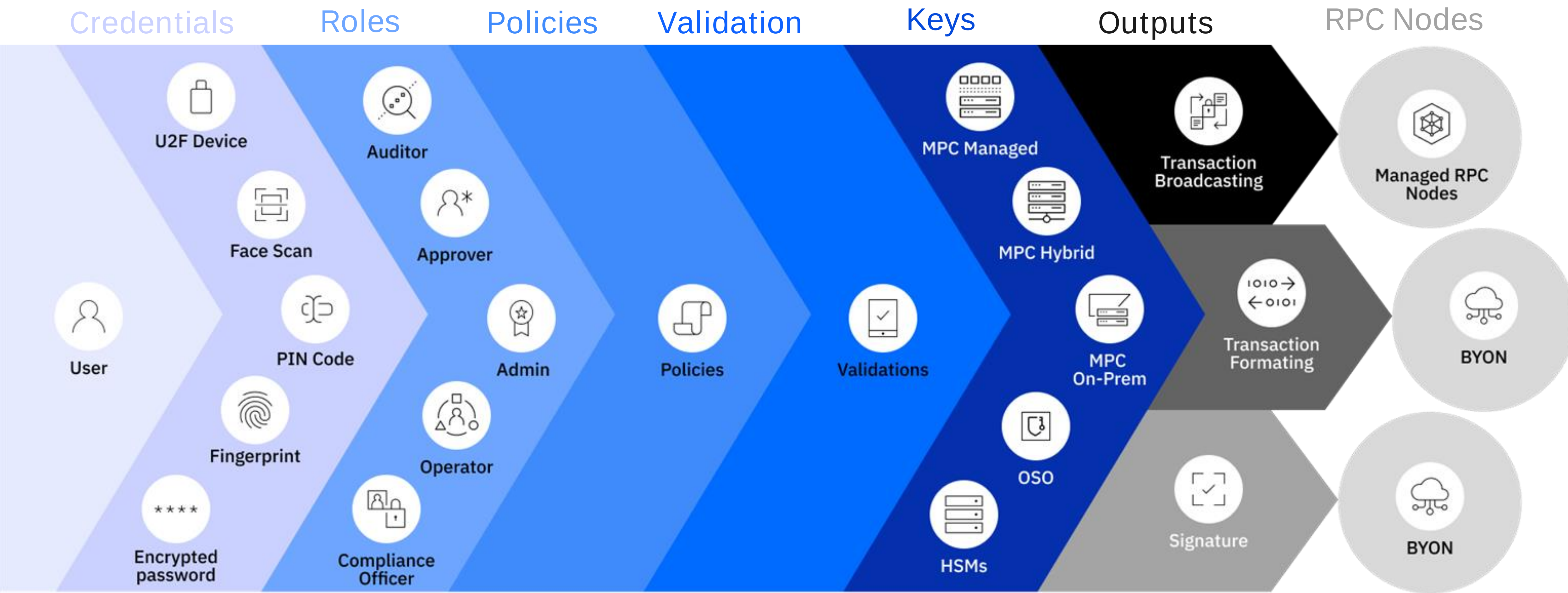
Cryptographic Agility
Support ECDSA, EdDSA/Schnorr, STARK, BIP/SLIP standards, and HD key derivation.

Certificates & Attestations
Attach immutable cryptographic logs and attestations to every signed request.

The secure & scalable foundation for your digital asset business



Transaction Lifecycle Overview



OSO = IBM Offline Signing Orchestrator
MPC = IBM Multi Party Computation
HSM = IBM Hardware Security Module
BYON = Bring your own nodes

Platform to control all onchain operations



Transaction
formatting



Webhook Alert



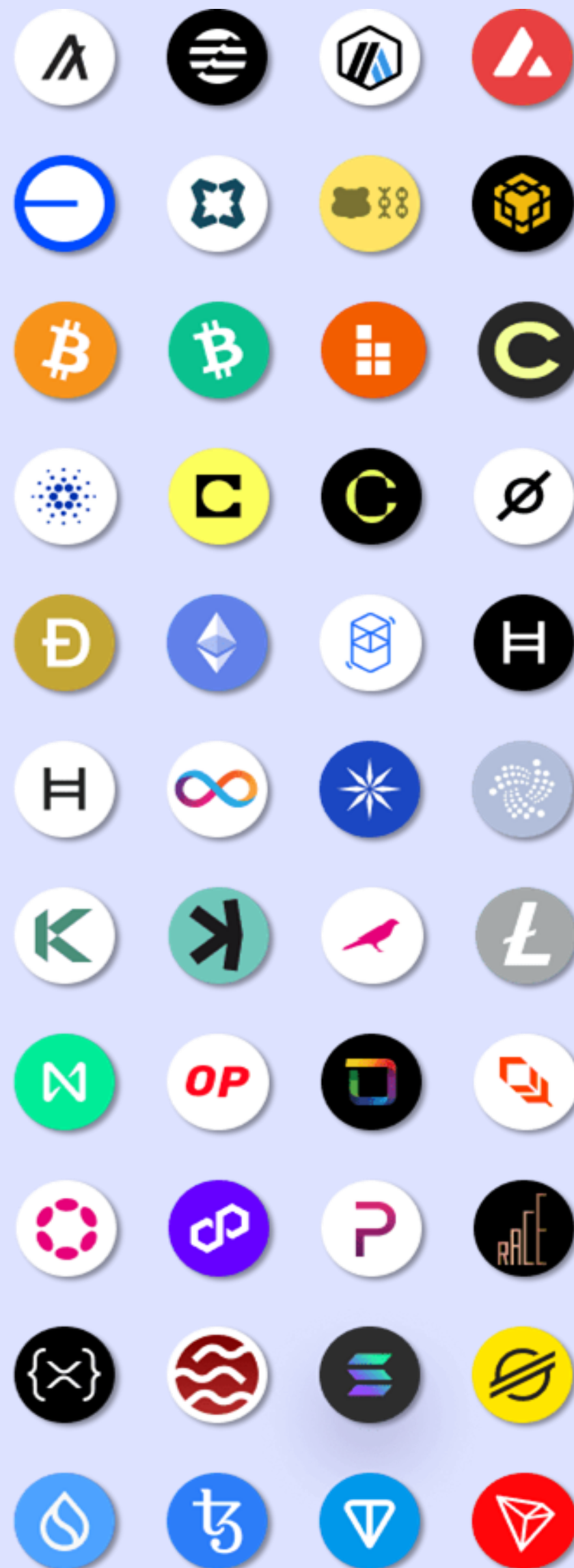
Indexing



Signing



Transaction
broadcast



Support for +40
blockchain
protocols

Transfer Assets [Simple & Easy]

- **Purpose** Best for straightforward token transfers
- **Abstraction** Provide basic details (sender, receiver, amount), and IBM handles the transaction.
- **Ease of Use** Ideal for common transfers with a simple interface.
- **Control** Limited control (e.g., cannot add custom data).

Broadcast Transaction [Flexible & Advanced]

- **Purpose** Used for complex transactions like smart contract interactions.
- **Control** Full control over onchain fees, limits, and custom data payloads.
- **Flexibility** Suitable for more advanced use cases and requires more technical knowledge.

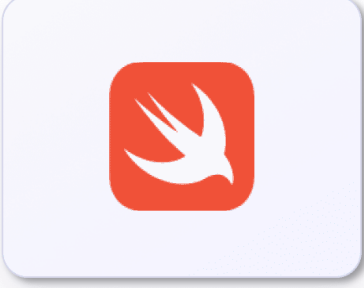
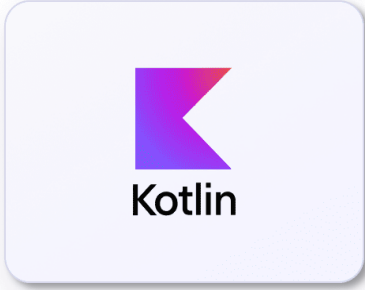
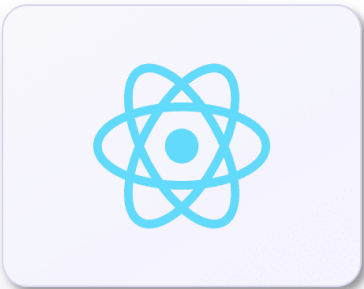
Generate Signature [Fully Autonomous]

- **Purpose** Used for complex transactions like smart contract interactions.
- **Control** Full control over onchain fees, limits, and custom data payloads.
- **Flexibility** Suitable for more advanced use cases and requires more technical knowledge.

Comprehensive suite of interfaces for admins & developers

SDK

API



Create a new user

```
1 {
2   "username": "MyNewUser@example.co",
3   "userId": "us-2mhcm-9190a-92ran47bjp160hmv",
4   "kind": "CustomerEmployee",
5   "credentialUuid": "cr-4uc9u-12ij1-9s08327e73jqcncr",
6   "orgId": "or-yanke-mars-6ulofamogg84s87v",
7   "permissions": [],
8   "scopes": [],
9   "isActive": true,
10  "isServiceAccount": false,
11  "isRegistered": false,
12  "permissionAssignments": []
13 }
14
```

IBM

Home

Funds

Transfers

Wallets

Organisation

Users

Policies

Keys

Settings

Home > Wallets

Main Treasury Wallet

USDC

Wallet ID 9359205940 04234 24

Address 0x0wefoak209g3m2...45e2

Net worth in USD \$4,230,703.34

Native Balance in Eth 19.4 Eth

Transactions 13

Assets

Asset	Balance	USD	Verified	Symbol	
Ethereum	13.4	234,203.00	✓	ETH	Send Stake
USDC	22600	22,600.00	✓	USD	Send Stake

Web

IBM

Wallets

Wallets

Wallets are collections of crypto accounts derived from the same seed.

Search...

Filter

Create a Wallet

Name	Networks	
Main Treasury Wall...	8	
USDC Wallet 1		
BTC wallet		

3 of 3 Wallets

Mobile
(end of 2025)

Audits, certifications & insurance

 SOC 2 Type I-II 2024 Deloitte. COMPLETED	 SOC 2 Type I 2025 KPMG COMPLETED	 SOC 2 Type II 2025 KPMG COMPLETED	 WebAuthn Working Group COMPLETED
 FROST NIST COMPLETED	 ISO 27001 KPMG COMPLETED	 ISO 27017 KPMG COMPLETED	 ISO 27018 KPMG COMPLETED
 Level 3 CCSS DigOpp ONGOING	 ISO 22301 MSECB ONGOING	 ISO 22380 MSECB ONGOING	 SOC 1 KPMG ONGOING

Certified SOC 2 Type II and ISO 27001, 27017, 27018



Pentested and audited by Yogosha, Halborn, Redacted and Kudelski



Insurance for crime, cyber and E&O



Third-party application integrations (existing & in-progress)

Exchanges

 Binance

 Gemini

 OKX

 Coinbase

 Kraken

 Bitstamp

Compliance

 Chainalysis

 Elliptic

 Scorechain

Yield & Staking

 Lido

 Nexo

 StakeWise

 Figment

 Matrixport

Swaps

 1inch

 Uniswap

 Matcha (by 0x)

Tokenization

 Polymesh

 Tokeny Solutions

 Securitize

 Linqto

Your future integrations (☺)

1



2



3



4



5



6



7



8



9



Core Banking

 Temenos

 Mambu

 Thought Machine

DeFi Tools

 Chainlink

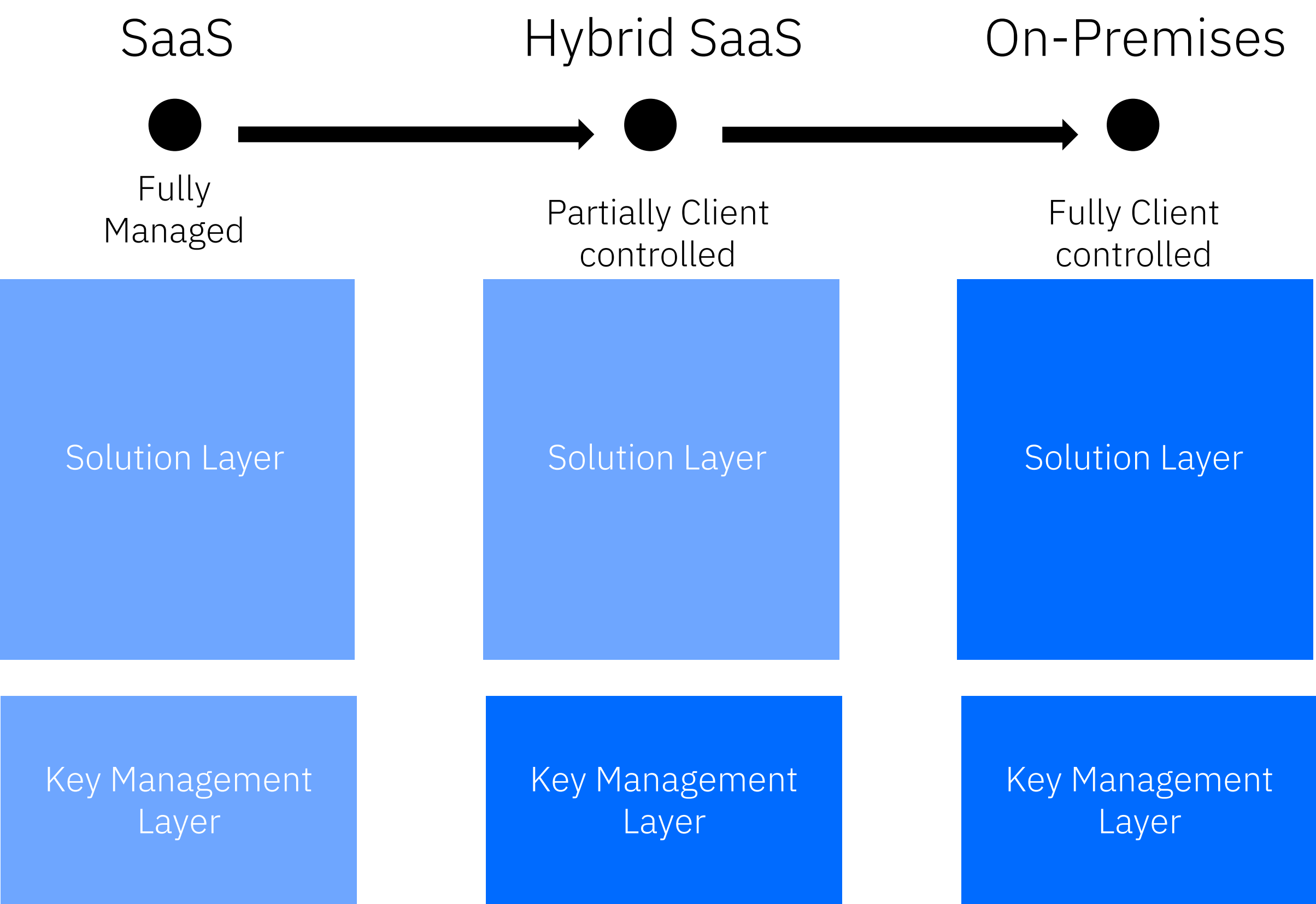
 WalletConnect

 0x Protocol

 DappRadar

Deployment options- & services

To meet regulatory requirements while enabling rapid time-to-market, IBM provides flexible deployment models with seamless upgrade paths.



SaaS & Hybrid will be available in Q4 2025. On-Premises in Q2 2026.

Cloud Client Data Center

Full support for Hybrid & On-Prem Deployments

Architectures: Proven default blueprints or fully customized designs.

On-site installation: Physical installation of IBM® LinuxONE.

Logical installations: Secure configuration of partitions of all environments (Prod, UAT, Test, Dev), secure enclave installations and deployment of IBM Digital Asset Haven.

Key ceremonies: Structured, auditable processes and documentation for key generation and management.

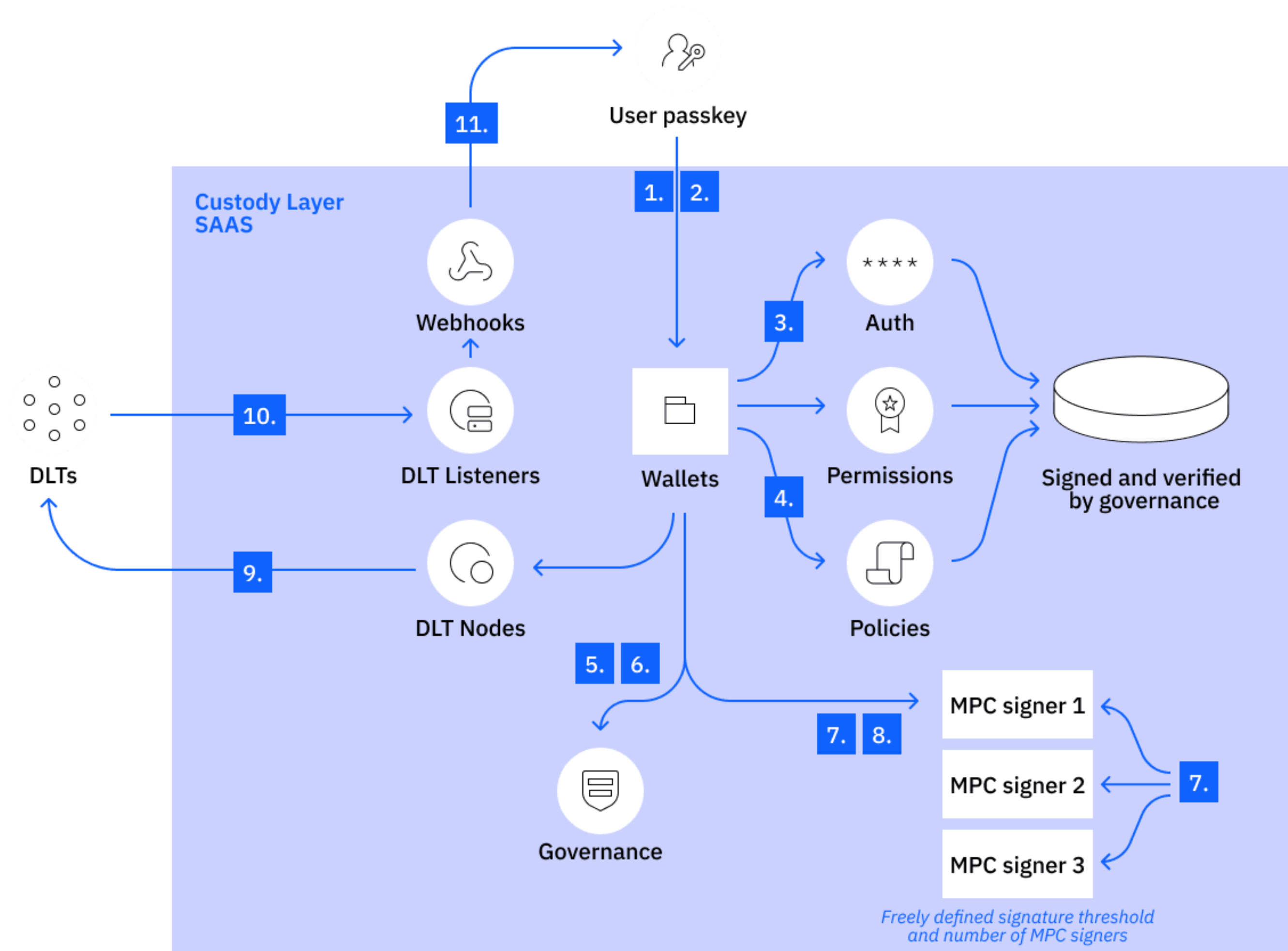
Enablement & handover: Knowledge transfer and best-practice guidance for smooth operations

Maintenance & support: Ongoing assistance, monitoring, and lifecycle management to ensure long-term reliability

Auditable hardware shipment: Tamper-proof, trackable delivery of IBM® LinuxONE.

Security architecture

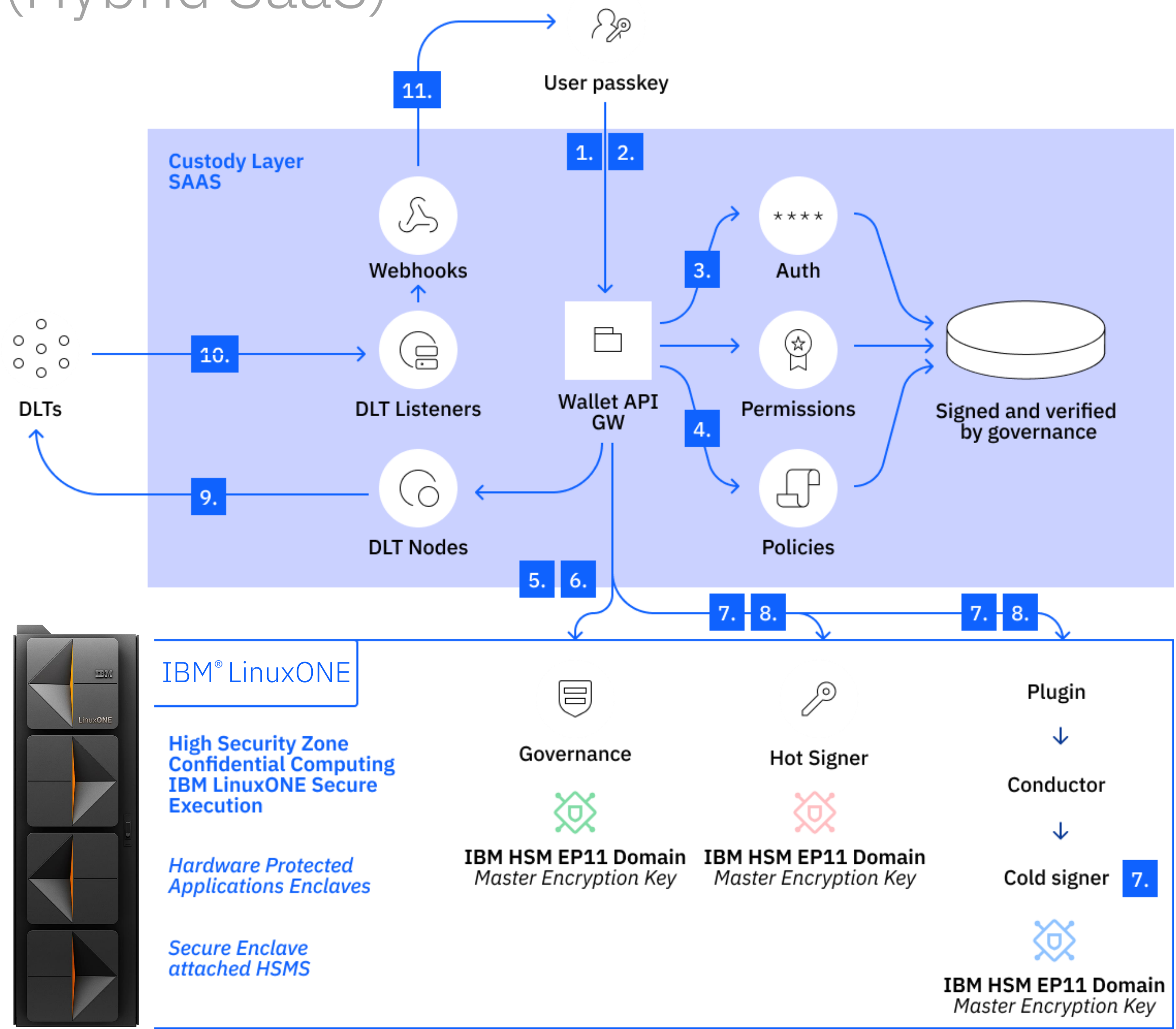
IBM Transaction Flow (Cloud SaaS)



1. User authenticates IBM SaaS using his/her passkey.
2. Users signs a transaction intent using his/her passkey and then submits the submit the tx intent
3. Auth and permissions verify the intent is signed by an authenticated user is authorized as per defined permissions.
4. Policies verifies defines policies rules are satisfied.
5. Governance retrieves the intent and verifies authentication, and permissions definition integrity. Governance engine verifies policies rules' integrity, and the approvals satisfy defined policies.
6. Governance forges the tx payload to be signed using the verified intent. Transaction payload is signed with its governance private key.
7. Each MPC signer retrieves the transaction payload and verifies governance signature and creates valid signature by communicating each other using the MPC protocol.
8. At the end of the MPC signing flow, the signed payload is sent to Wallet.
9. Transaction is broadcasted to DLT using IBM nodes.
10. Listeners monitors that the transaction has been written onto DLT.
11. When transaction is written on DLT, event is sent to the user.

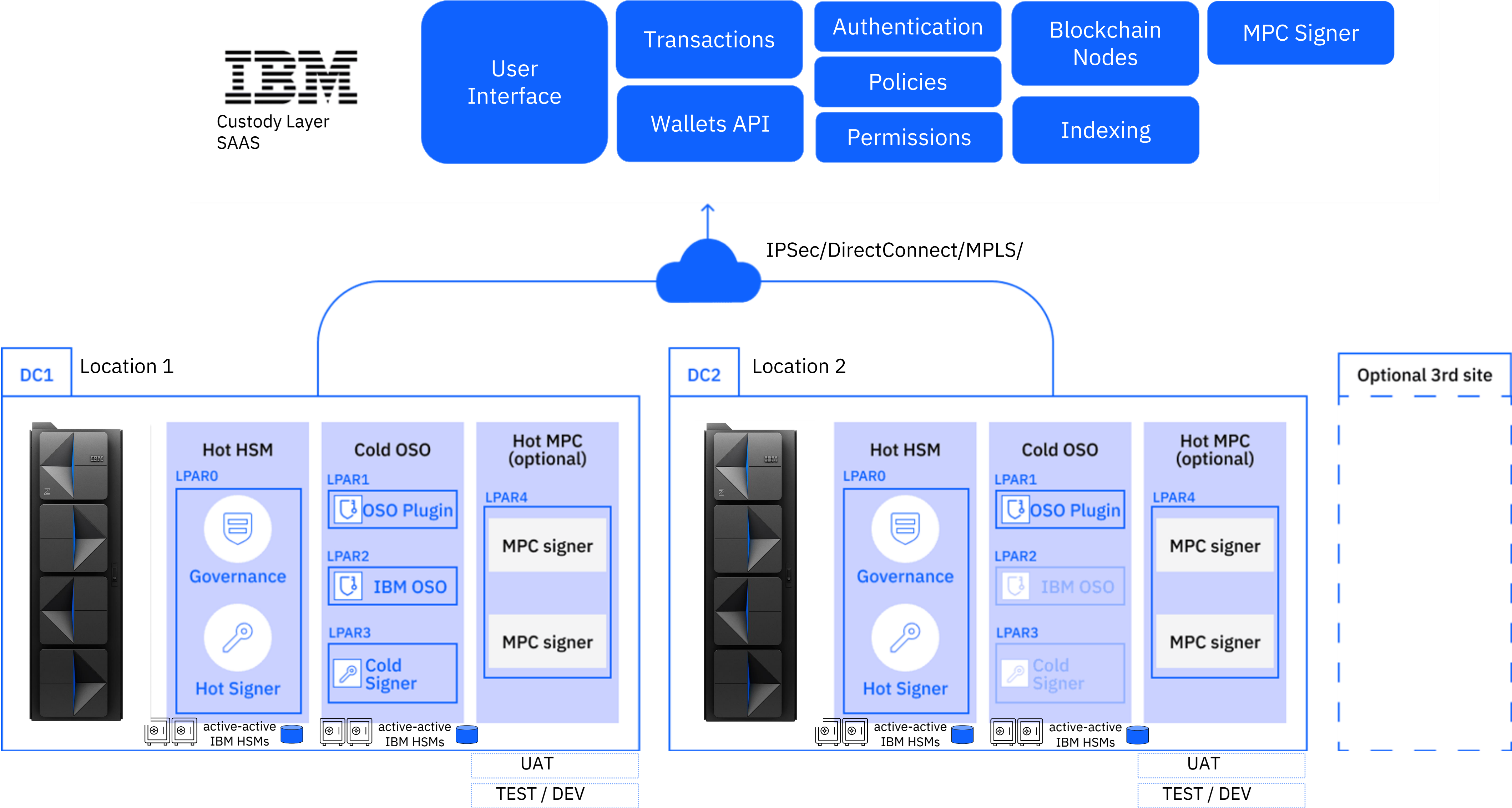
IBM Transaction Flow

(Hybrid SaaS)



1. User authenticates IBM SaaS using his/her passkey.
2. Users signs a transaction intent using his/her passkey and then submits the submit the tx intent
3. Auth and permissions verify the intent is signed by an authenticated user is authorized as per defined permissions.
4. Policies verifies defines policies rules are satisfied.
5. Governance retrieves the intent and verifies authentication, and permissions definition integrity. Governance engine verifies policies rules' integrity, and the approvals satisfy defined policies.
6. Governance forges the tx payload to be signed using the verified intent. Transaction payload is signed with its governance private key.
7. Signer retrieves the transaction payload and verifies governance signature. Then signer signs transaction payload with asset private key.
8. Signed payload is uploaded to IBM SaaS.
9. Transaction is broadcasted to DLT using IBM nodes.
10. Listeners monitors that the transaction has been written onto DLT.
11. When transaction is written on DLT, event is sent to the user.

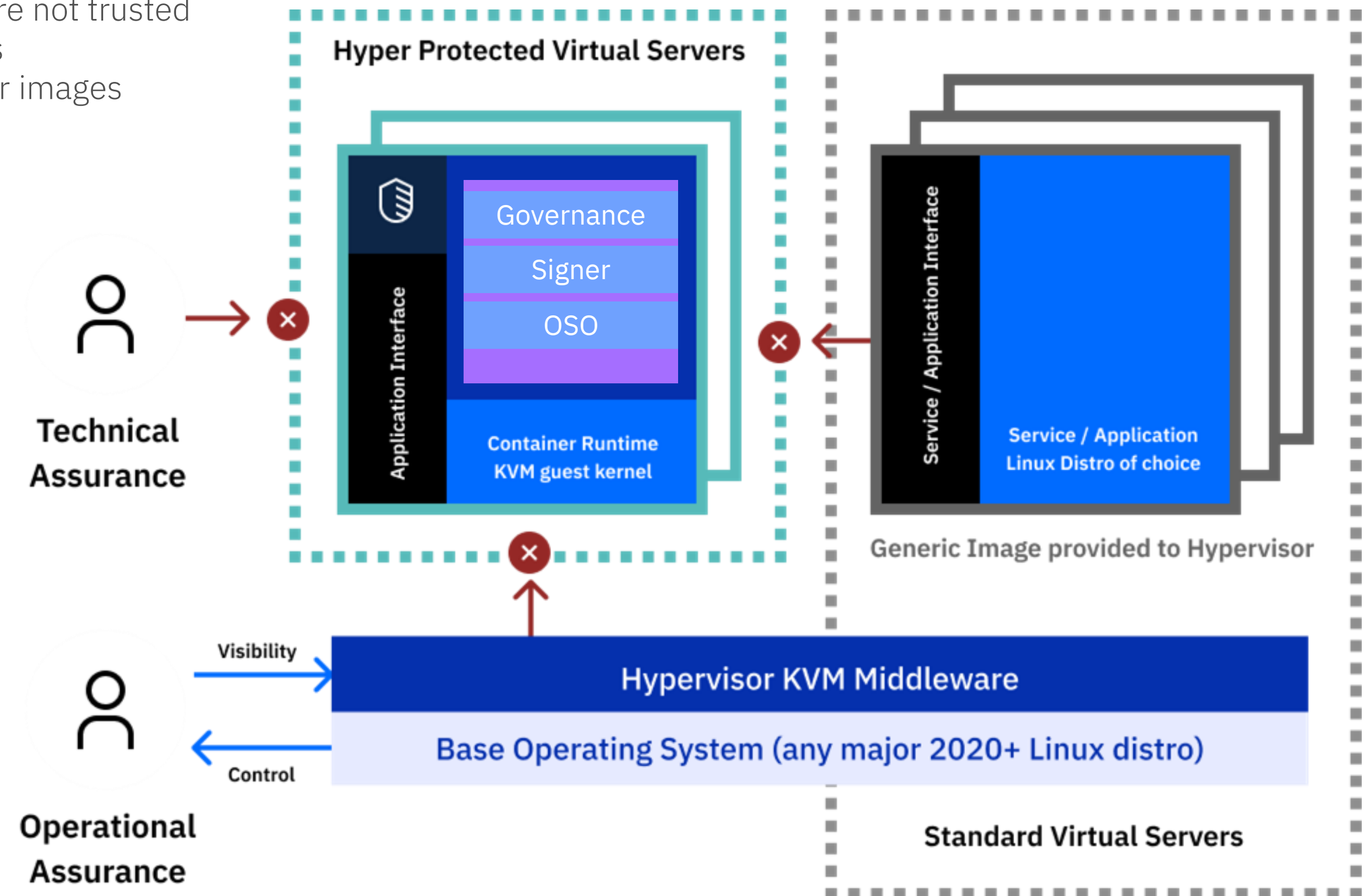
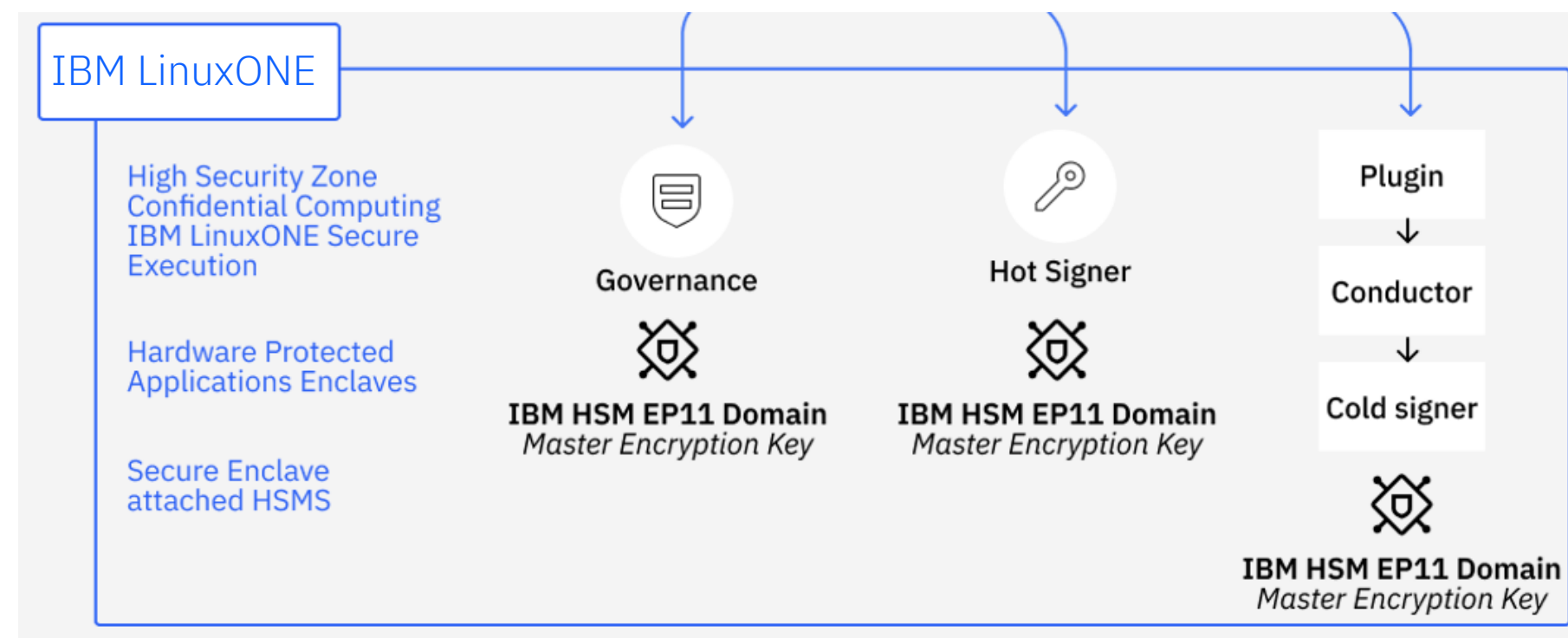
Deployment architecture for Hybrid SaaS



Protecting critical components on-premises (Hybrid SaaS)

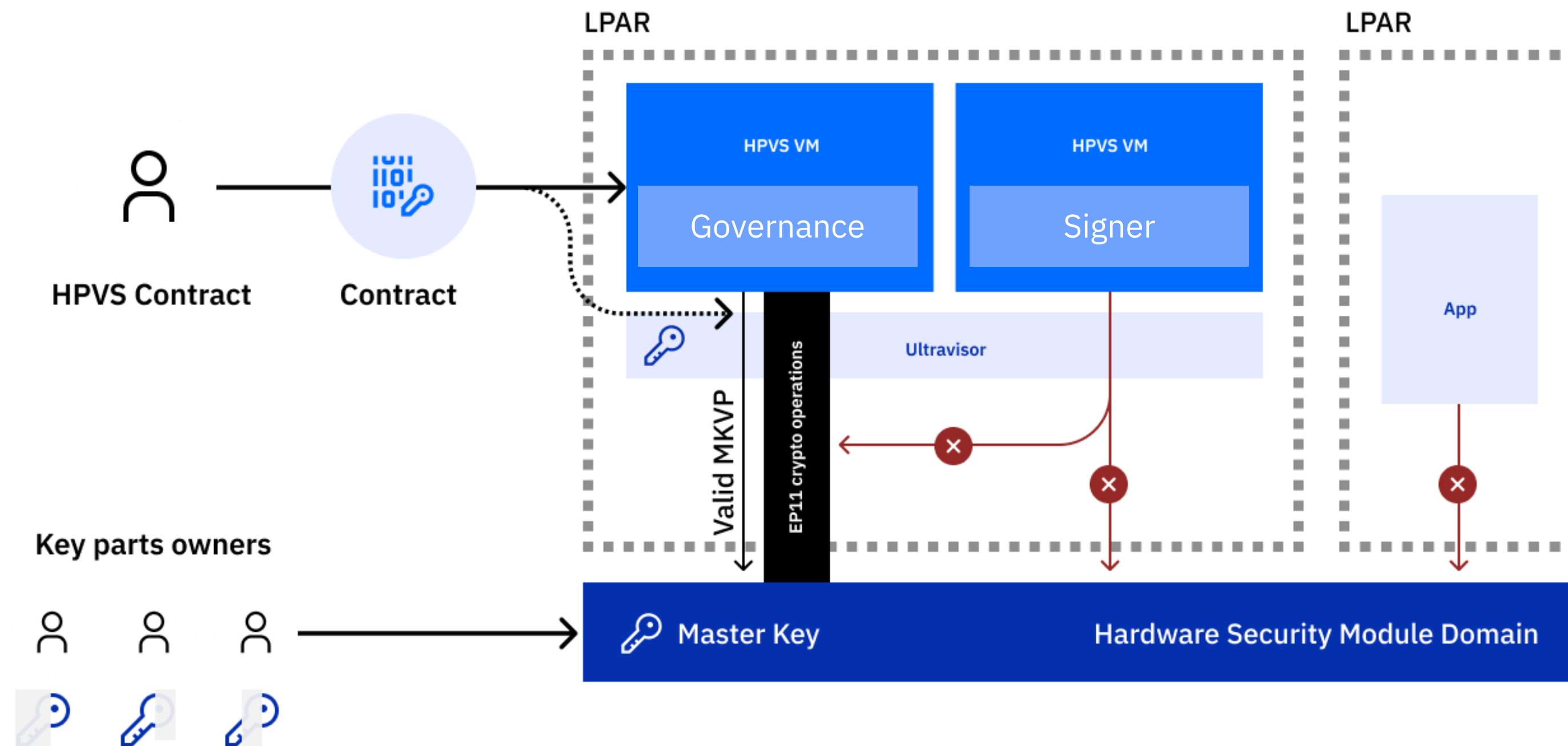
Hardware-based secure enclaves ensure privileged admins cannot bypass or tamper the governance, signers or cold storage orchestration.

- No command line or SSH
- No direct operating system access
- Code & data encrypted in flight & at rest
- Cannot access memory
- Administrators are not trusted
- No code changes
- Encrypt container images



Leveraging “IBM Crypto Passthrough”

Benefits of implementing Hybrid SaaS



Ultravisor memory is tagged such that the CPU can only access the ultravisor memory if it is in an UV-state.

Only ultravisor working on behalf of a specific secure guest can access the memory containing the secret as the memory storing the association secret is tagged. The Secret is placed in Memory that cannot be dumped during a system dump.

The IBM Z & IBM® LinuxONE memory is encrypted by a random key generated at IML.

Technology leveraging IBM Z & IBM® LinuxONE hardware capabilities

IBM's statement of direction:
Crypto Express8S Enablement for IBM®
Secure Execution for Linux®.

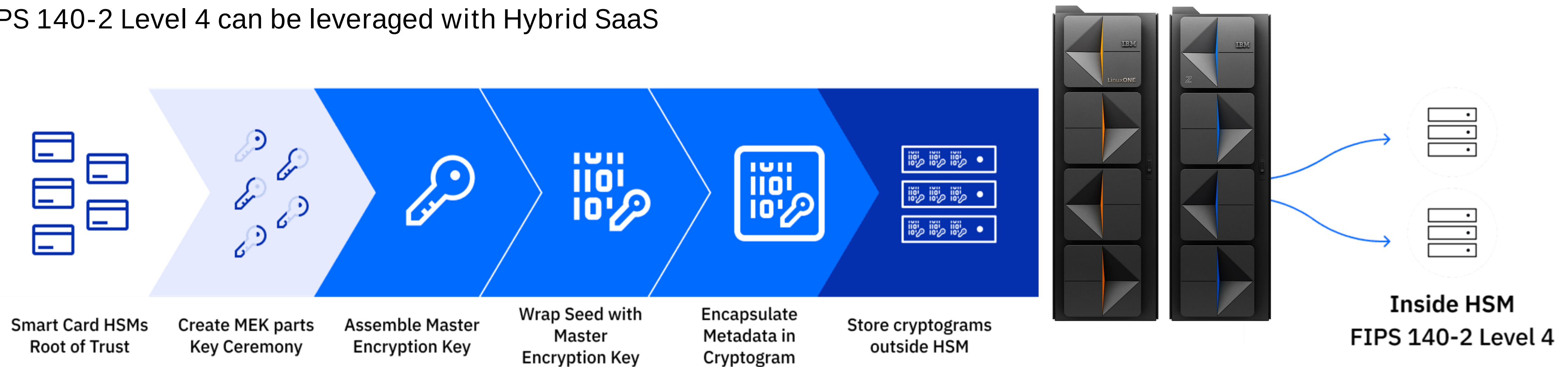
Crypto Passthrough consists of:

- A new function to assign Crypto adapters to IBM Secure Execution guest for Linux.
- Cryptographically binding all secure-key objects created by the secure guest such that the secure-key objects are only usable by the secure guest.

Supported Key Management

Industry's highest rated security & unlimited wallet scaling

IBM's CryptoExpress 8S HSMs, embedded in IBM® LinuxONE & IBM Z FIPS 140-2 Level 4 can be leveraged with Hybrid SaaS



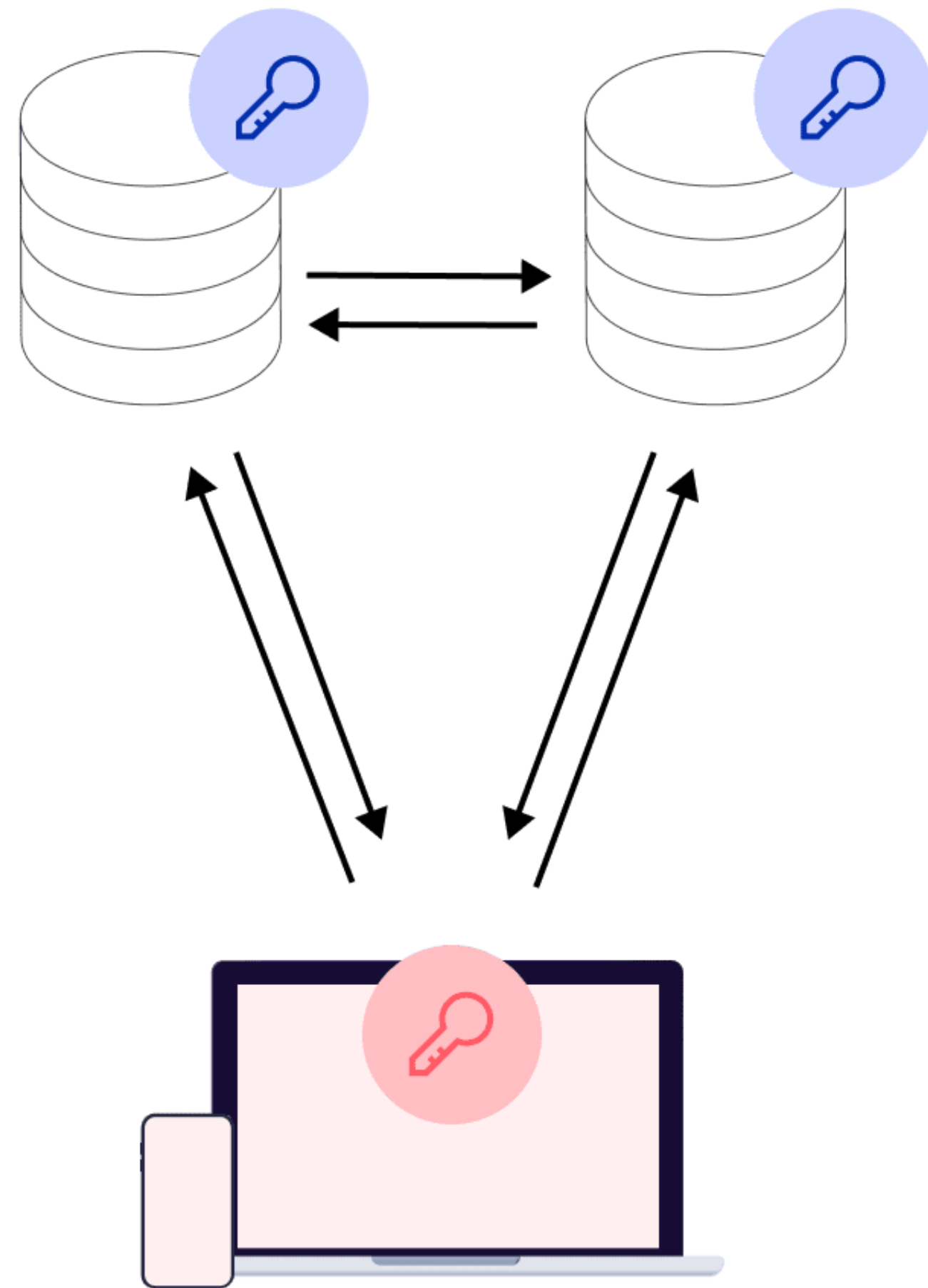
Master Encryption Key

- Encrypt and decrypt an unlimited number of Private Keys (Limitless Scale)
- Non-extractable stateless key

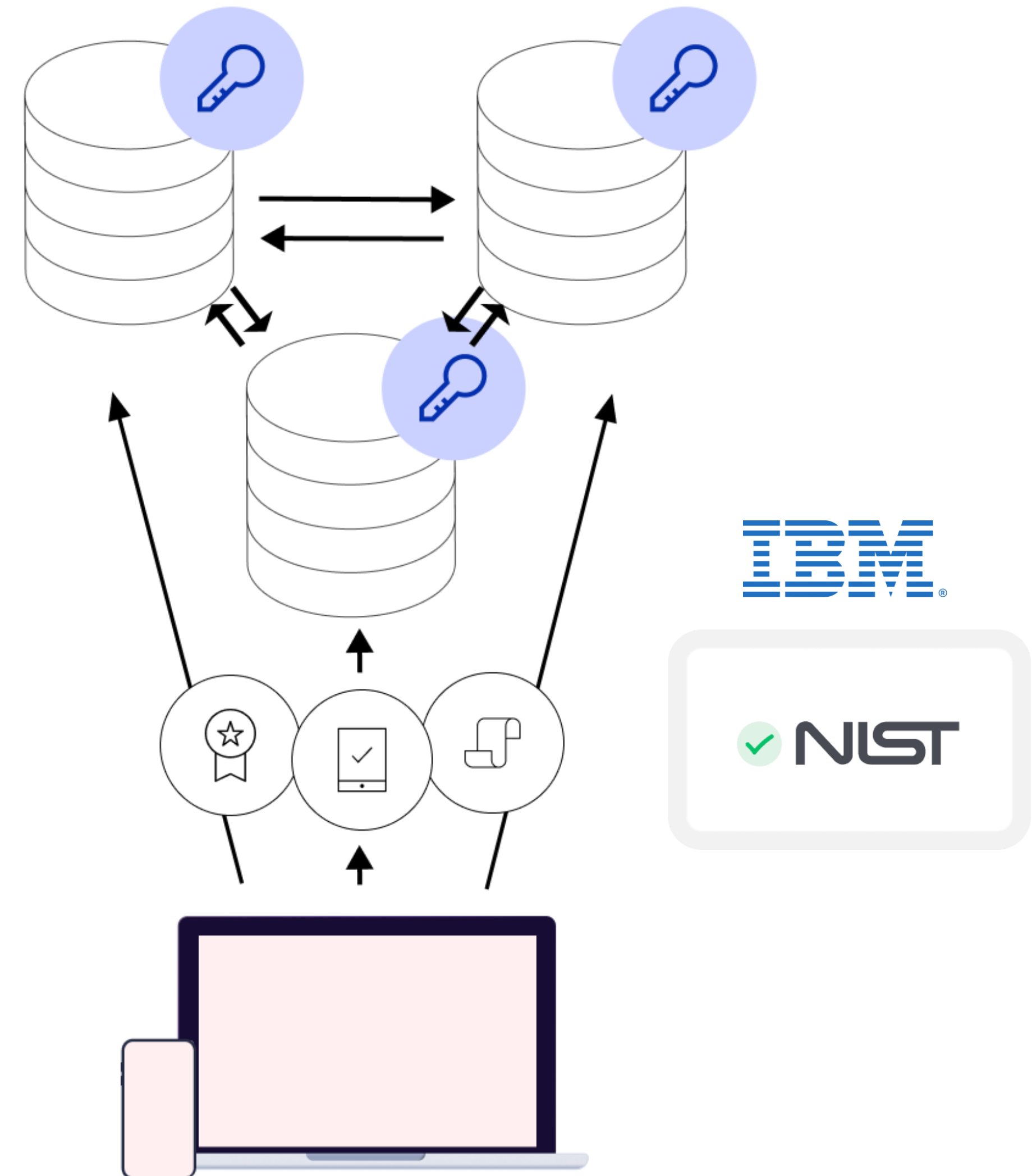
Cryptograms

- Binary objects
- Encrypted Hierarchical deterministic speed
- Stored commonly in databases in enclaves, back-up and distribution benefits

User-hosted versus Network-hosted Multi-Party Computation



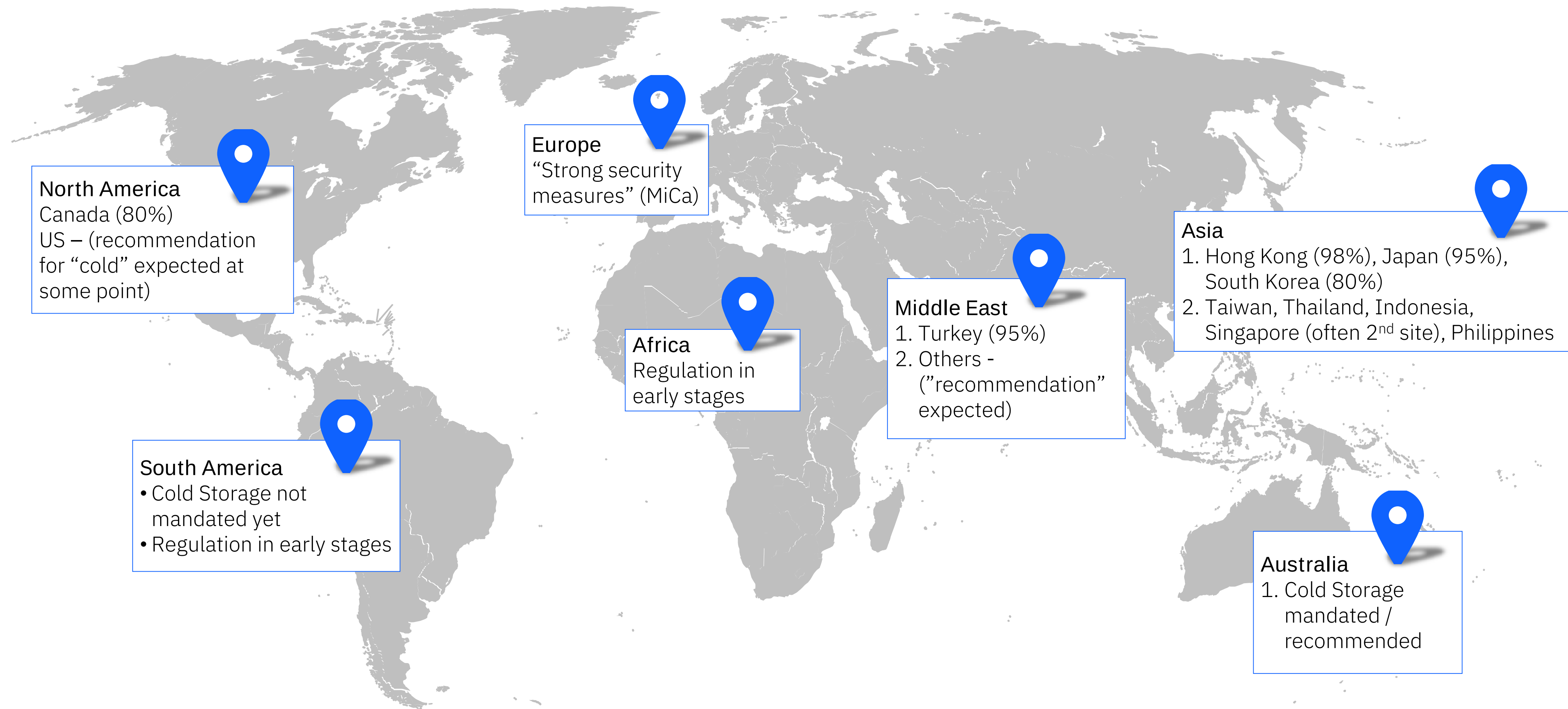
Conventional model



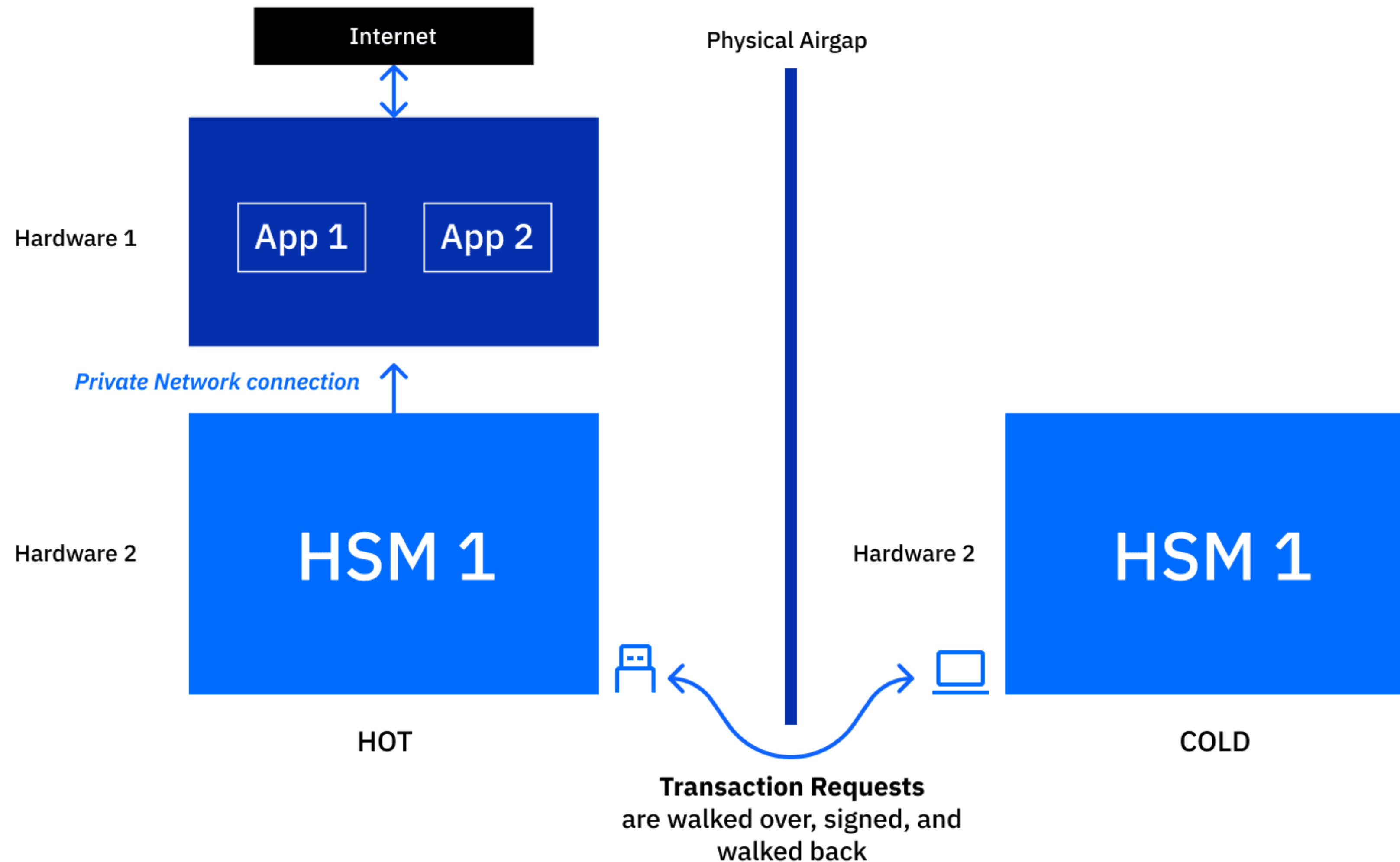
Proposed model

Keeping assets offline (“cold”)

First regulations enforce custodians to keep digital assets offline / dis-connected; asset insurance is cheaper for “cold”

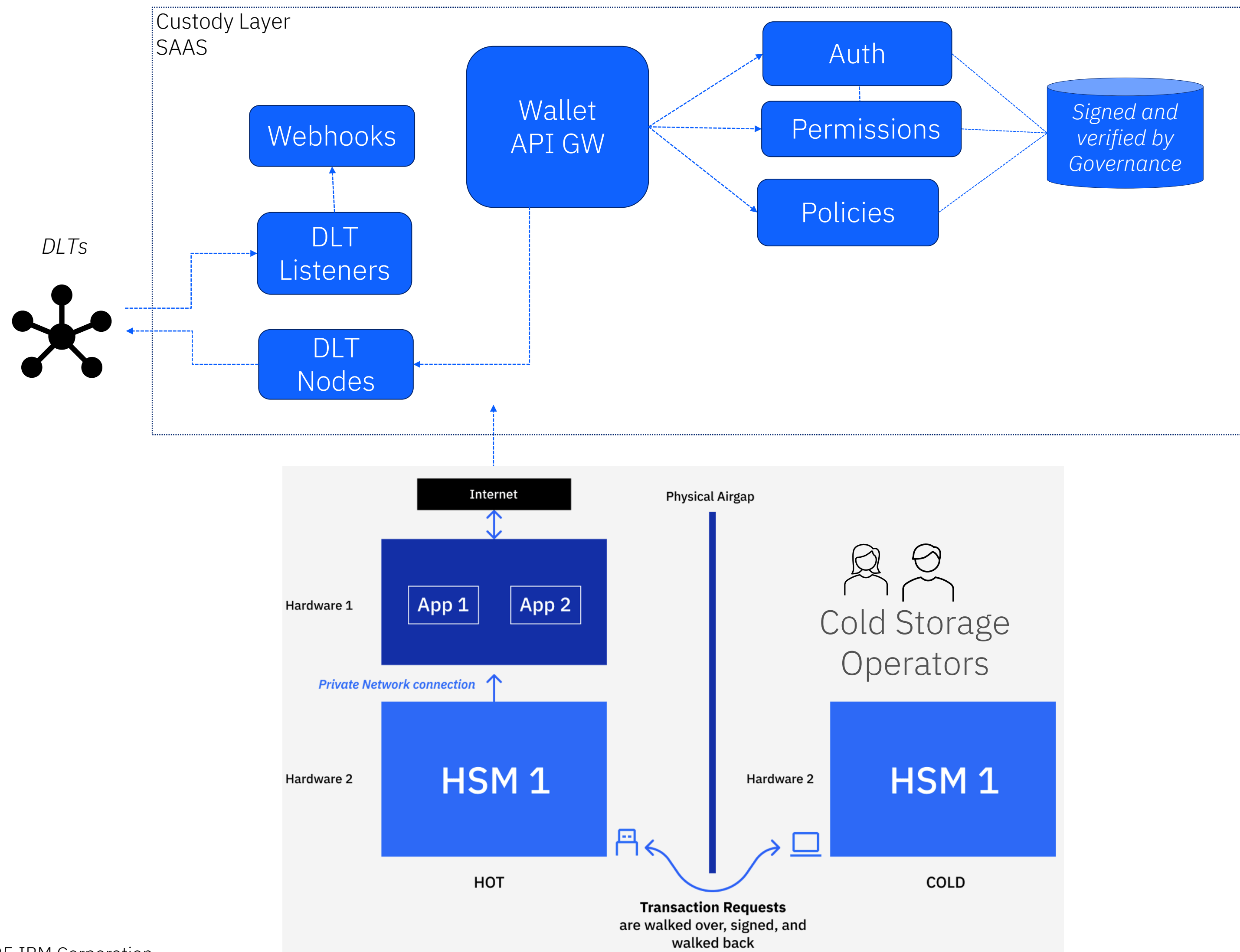


Traditional cold storage approaches have their challenges & downsides (1/2)



- Humans are involved in the operation
- Introduction of untrusted devices for data transfer (or even key shard storage)
- Manual operation required, risk for operational errors
- Bank "owns" the process (audit) and the responsibility
- Scalability is limited
- Client Service is limited
- No strong protection against forced attacks

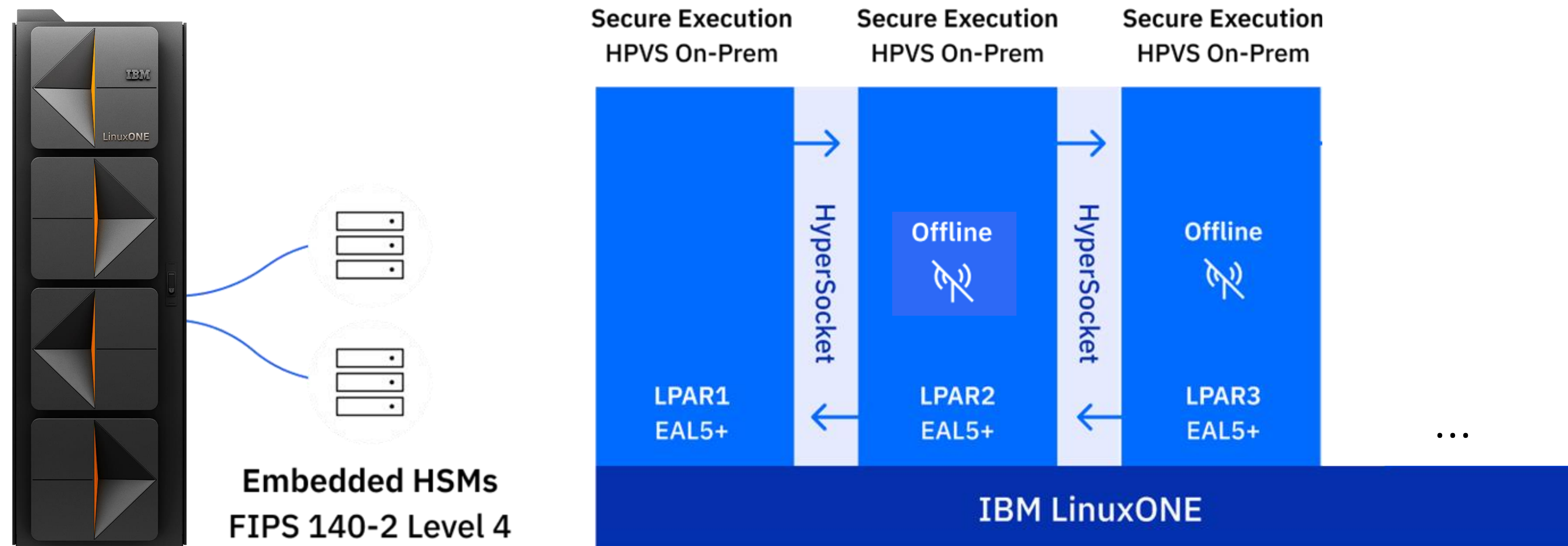
Traditional cold storage approaches have their challenges & downsides (2/2)



Cold Storage Operators need to trust the custody core layer was not manipulated.

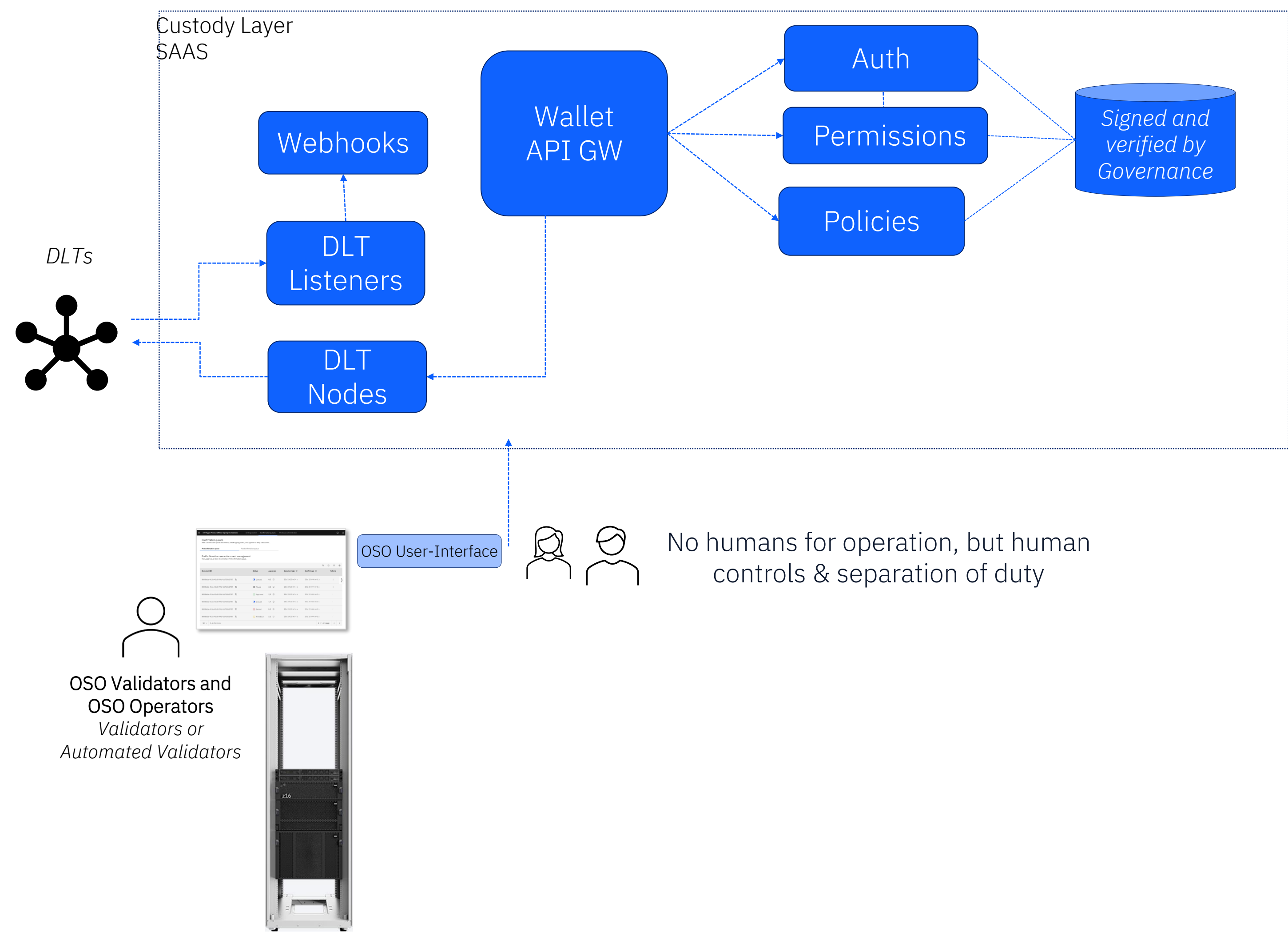
- Trust that the number of approvers wasn't changed.
- Trust that approvers reviewed correctly.
- Trust that the UI was not manipulated.

Ingredients for an enterprise-grade, policy-driven, locked-down, cold storage orchestration

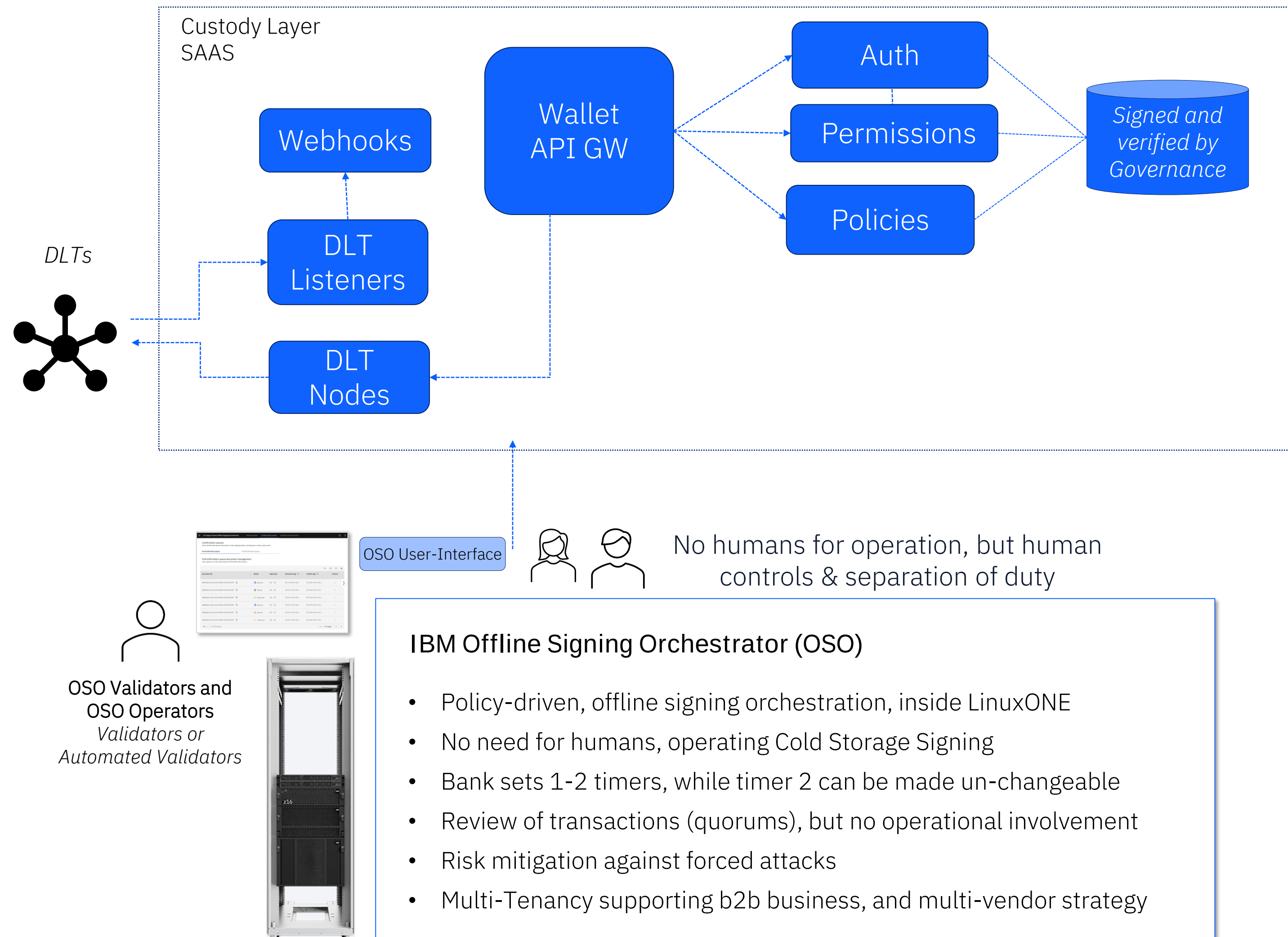


1. Better than airgapped isolation between partitions as no network attack vector
2. Encrypted, in-memory, uni-directional communication instead of using cables as with traditional cold storage
3. LPARs can be configured without network switches and be completely offline, airgapped, disconnected
4. LPARs and embedded HSMs can be powered off and made unavailable
5. Privileged Administrators cannot swap out or manipulate images within LPARs or manipulate the deployment

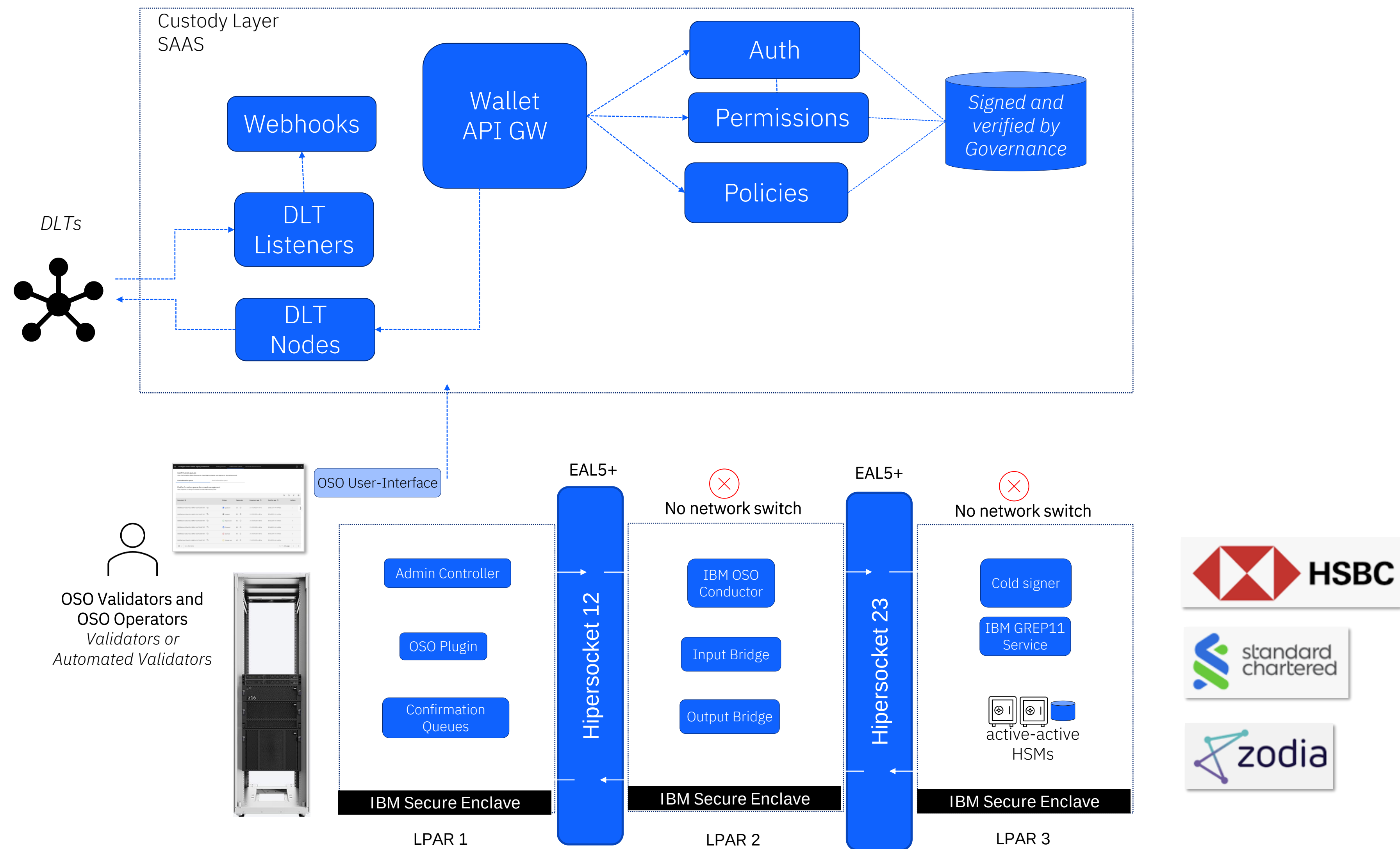
IBM Offline Signing Orchestrator (OSO) addresses traditional challenges



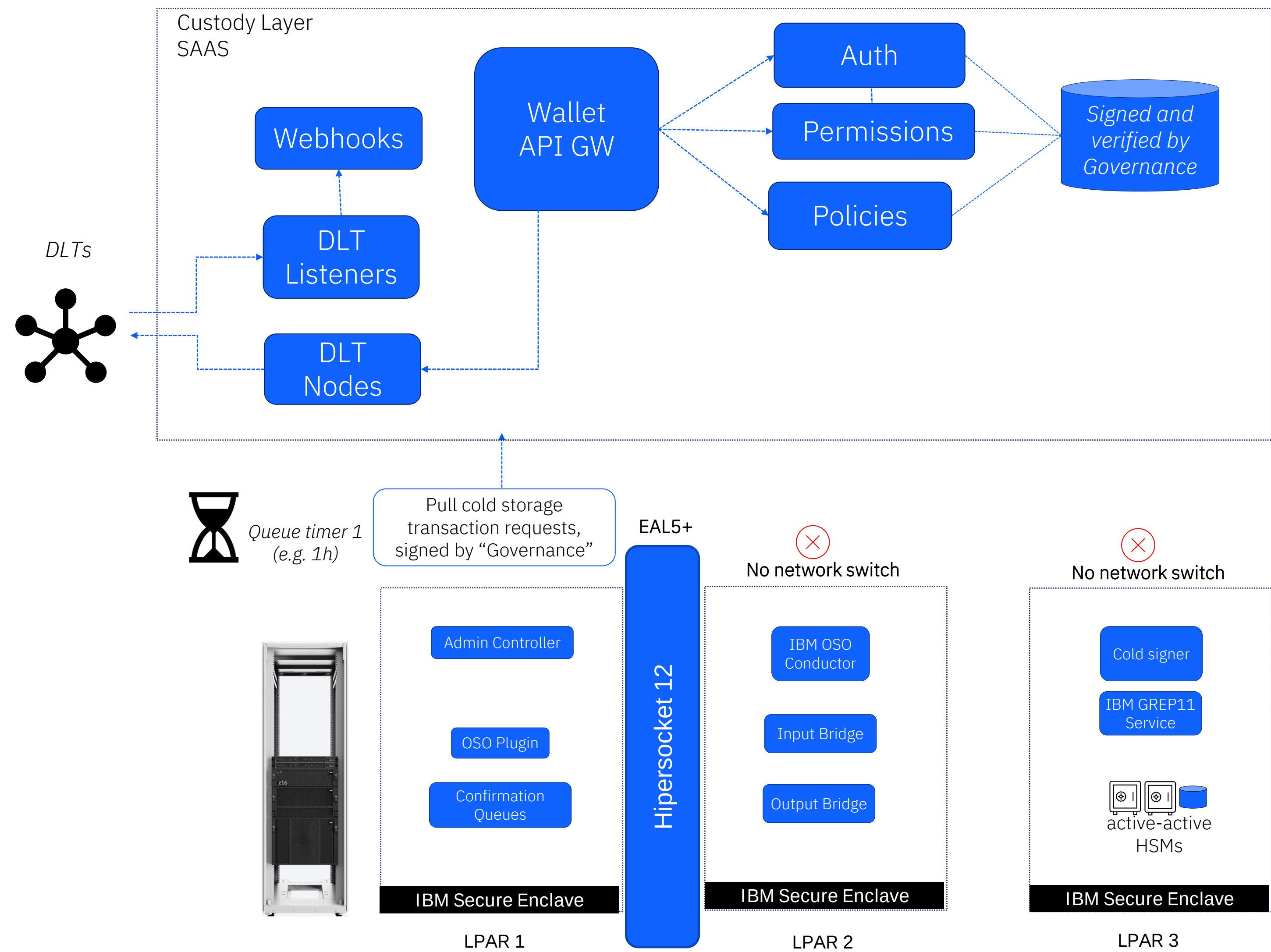
IBM Offline Signing Orchestrator (OSO)



IBM Offline Signing Orchestrator (OSO)

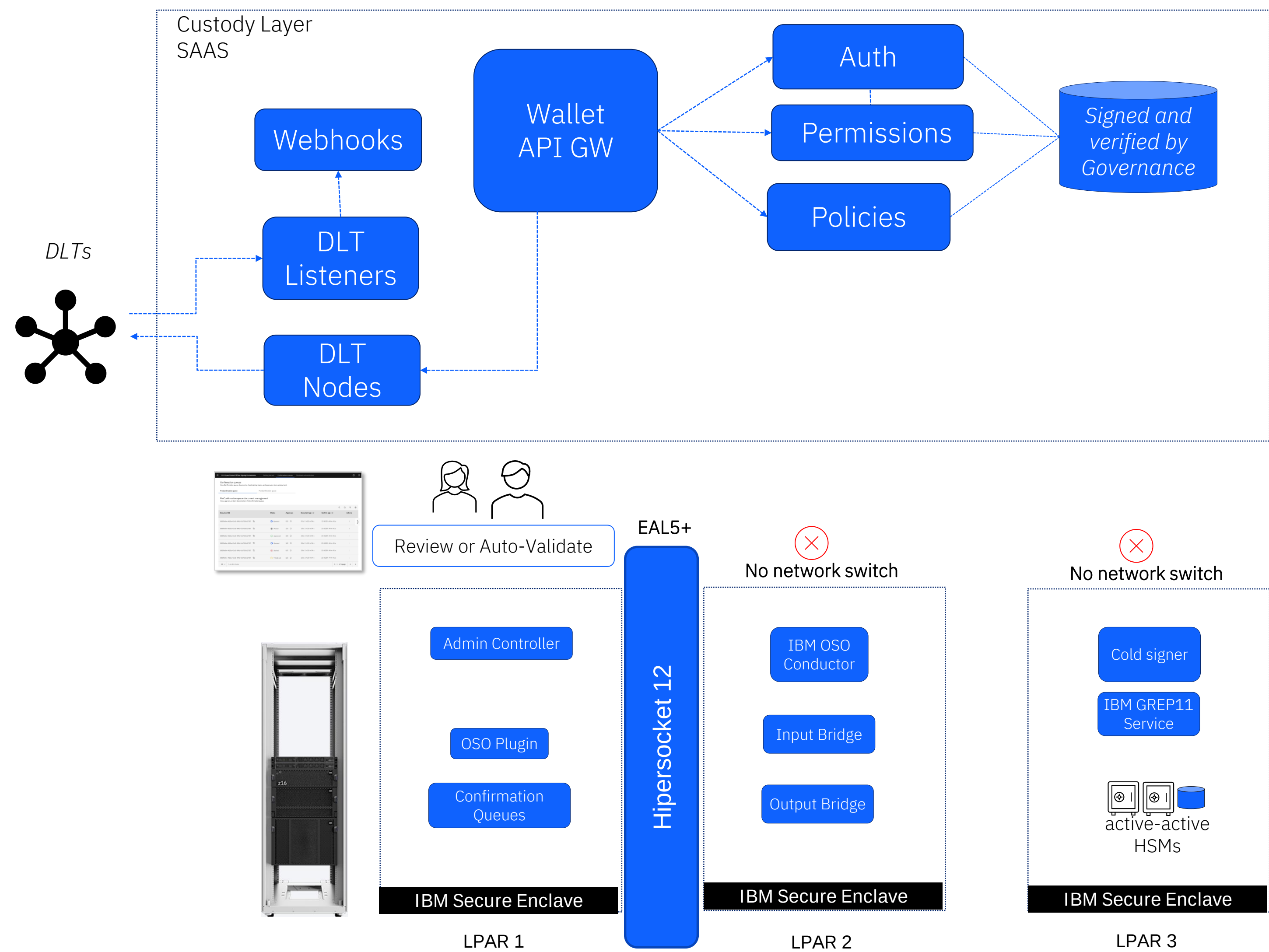


Cold Storage Signing Flow



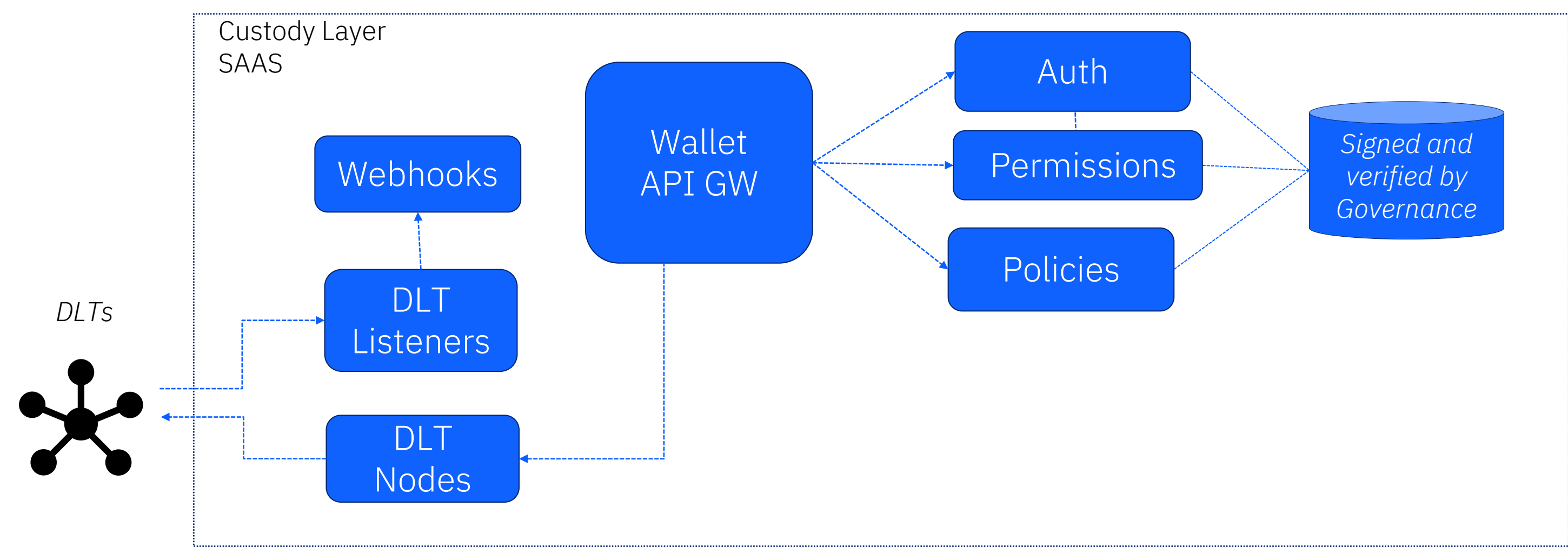
1

Cold Storage Signing Flow

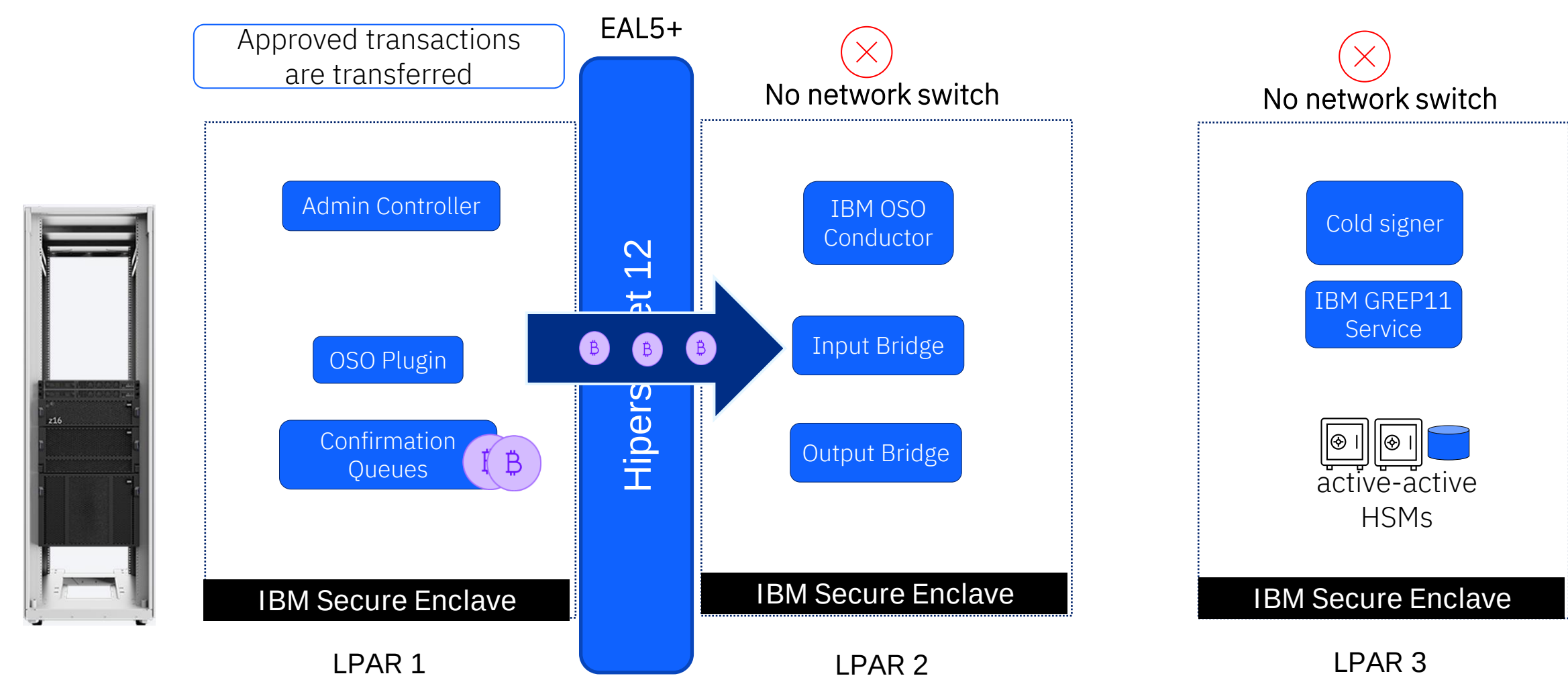


2

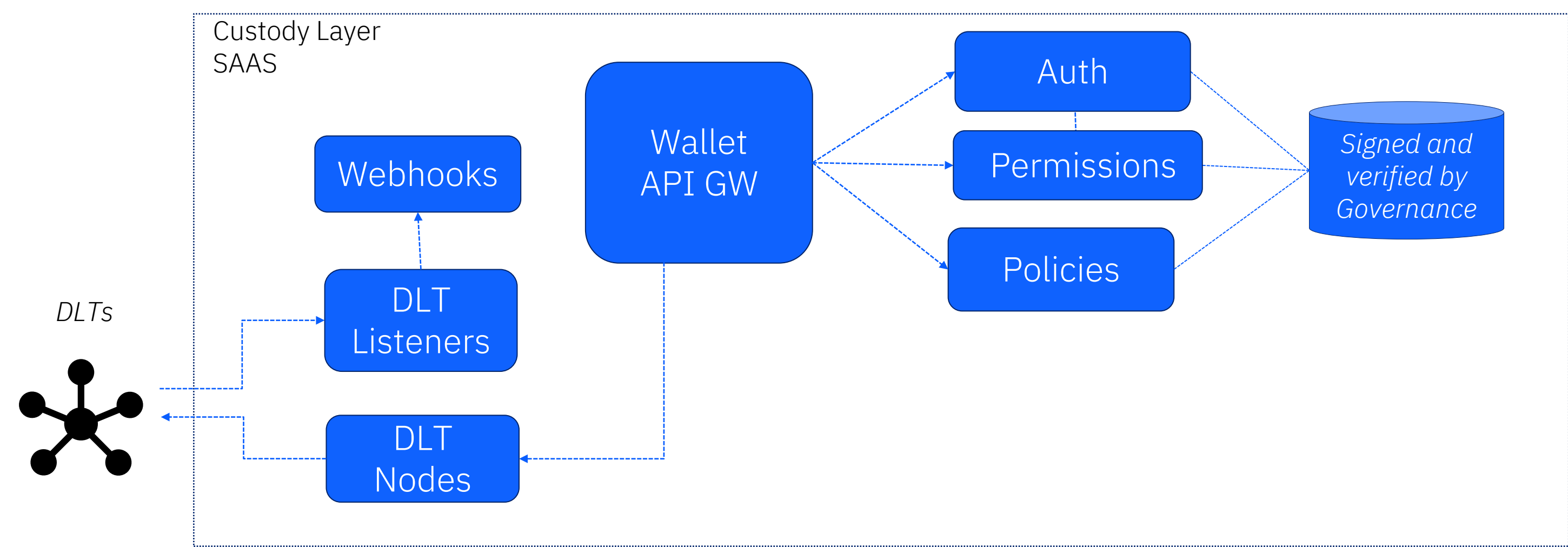
Cold Storage Signing Flow



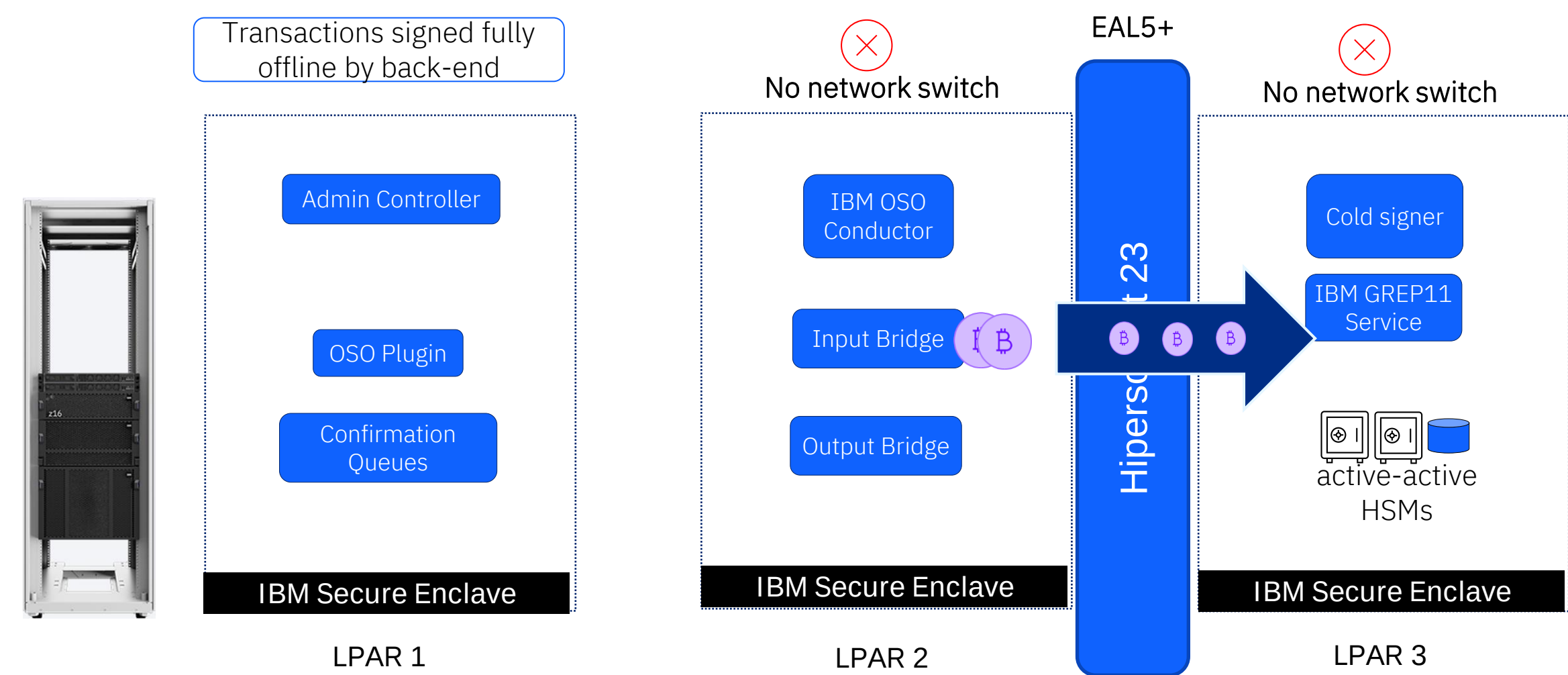
3



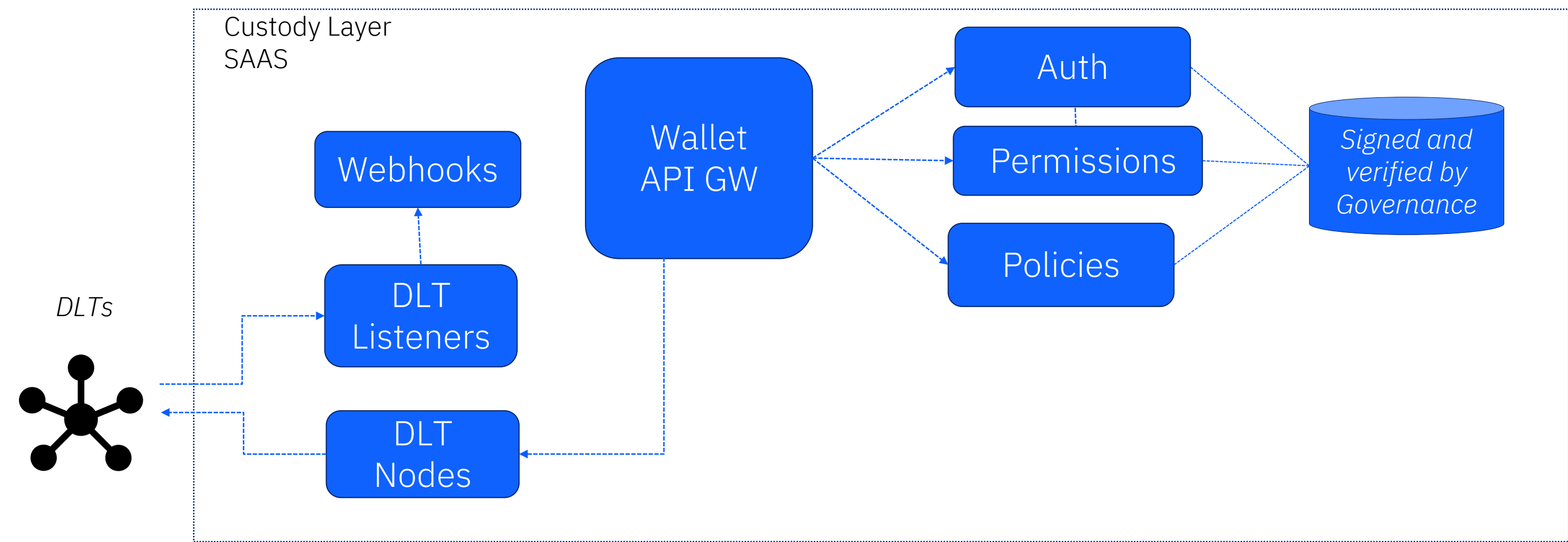
Cold Storage Signing Flow



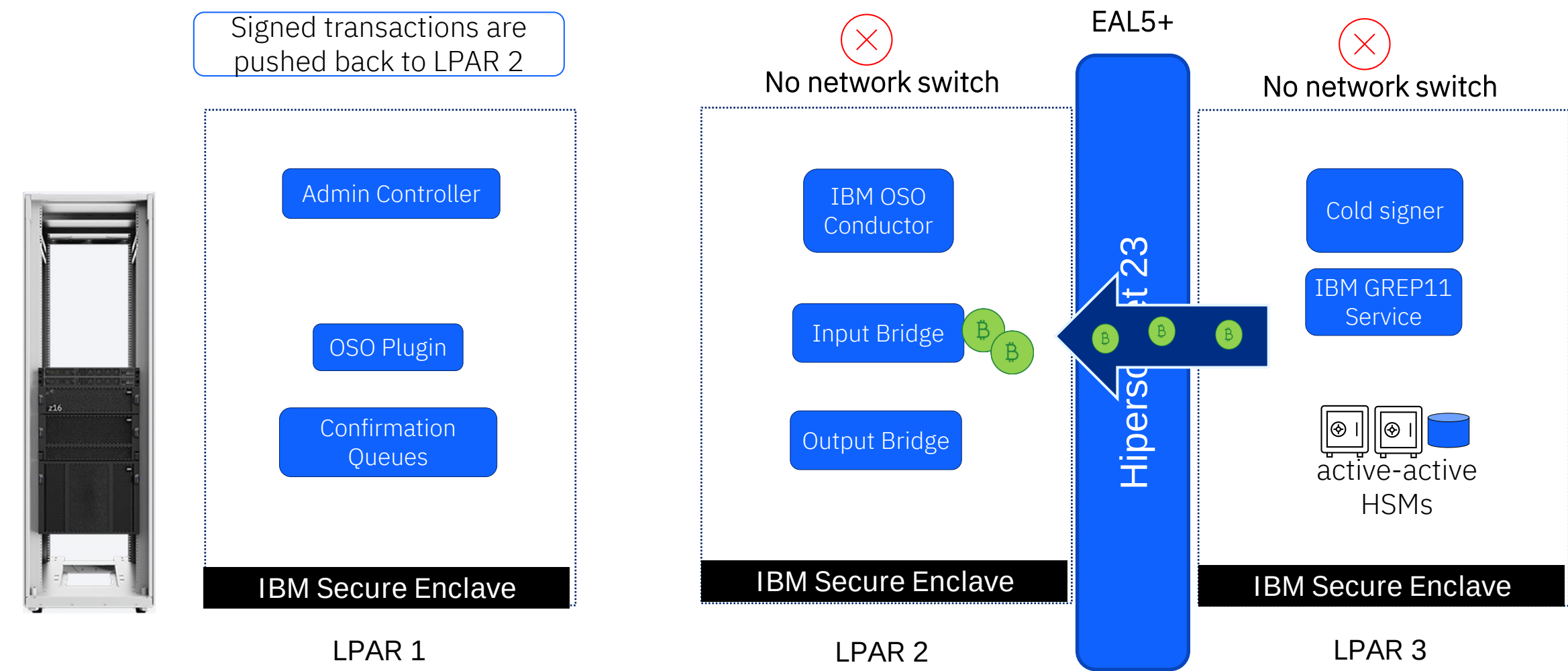
4



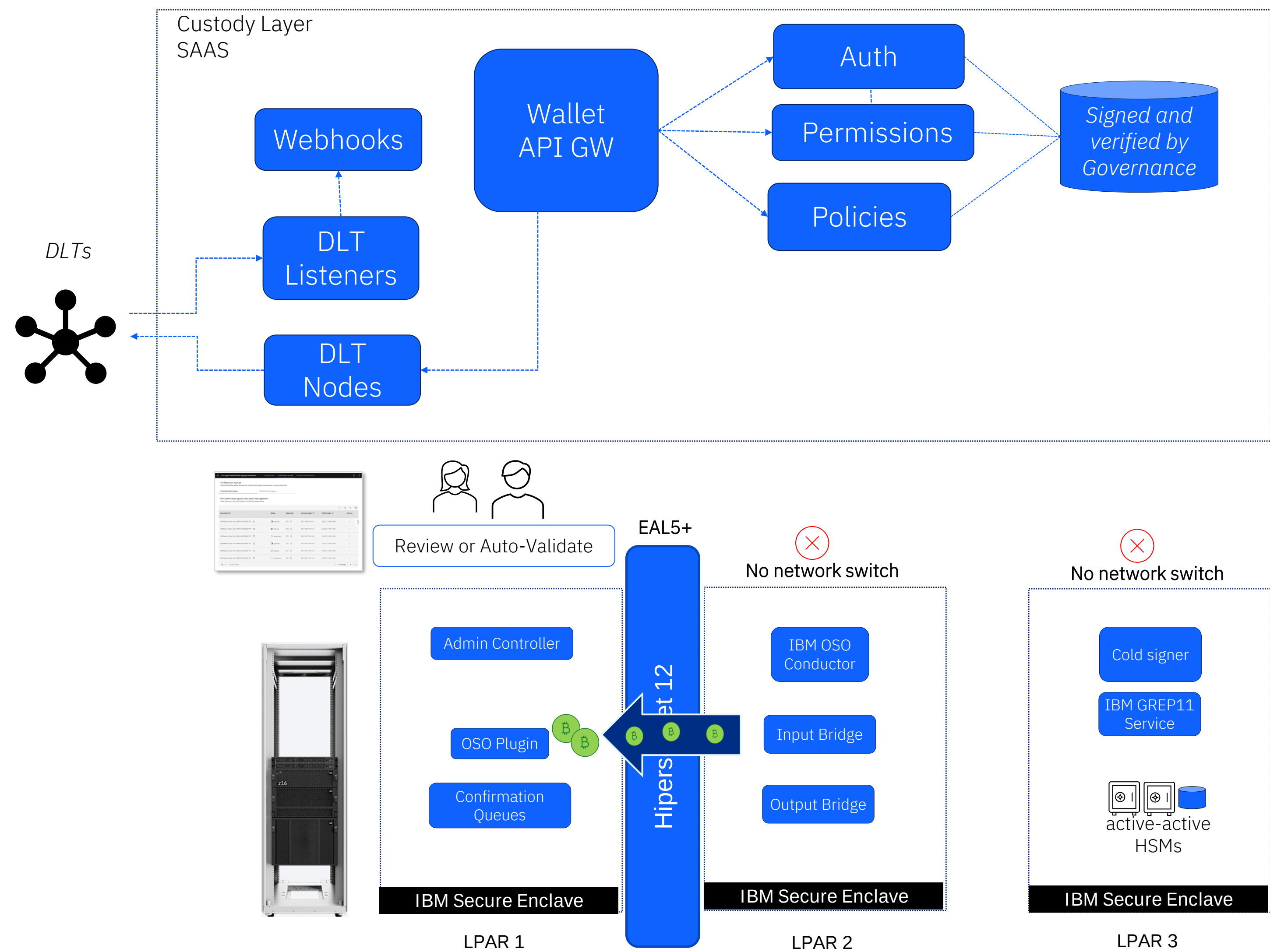
Cold Storage Signing Flow



5

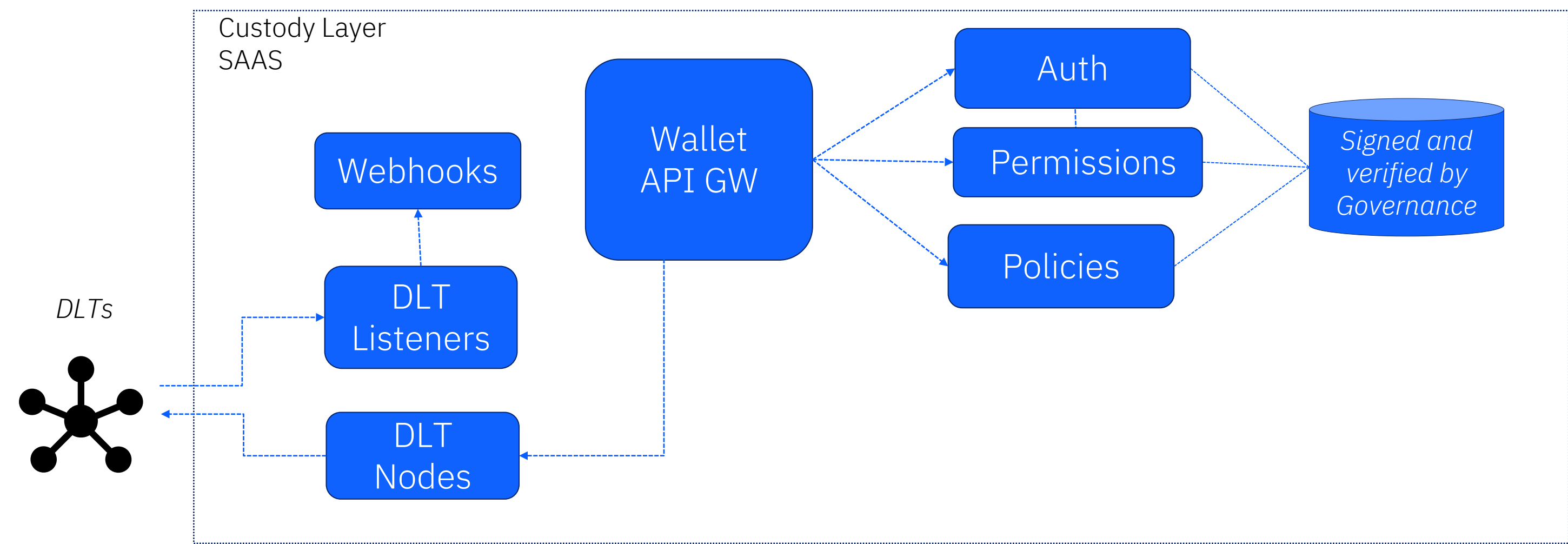


Cold Storage Signing Flow

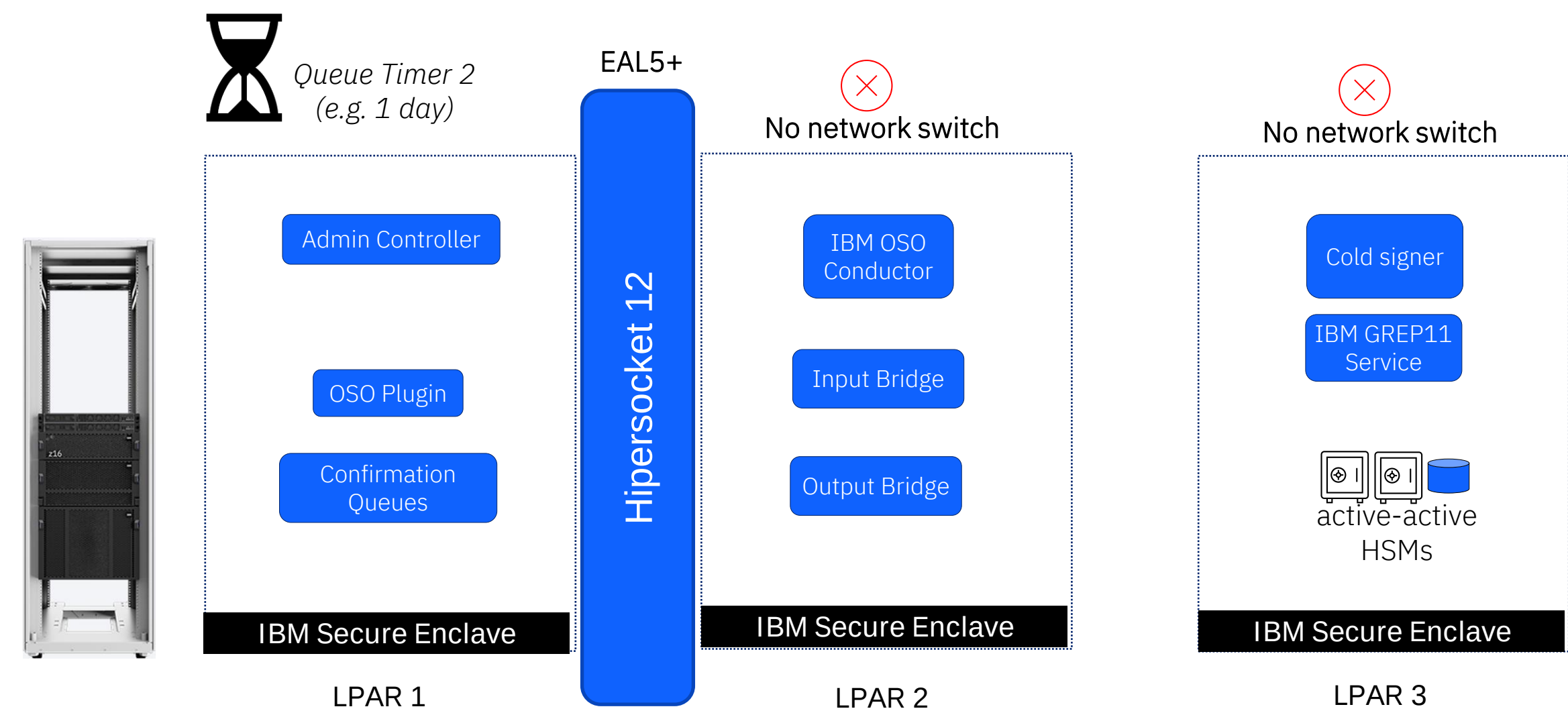


6

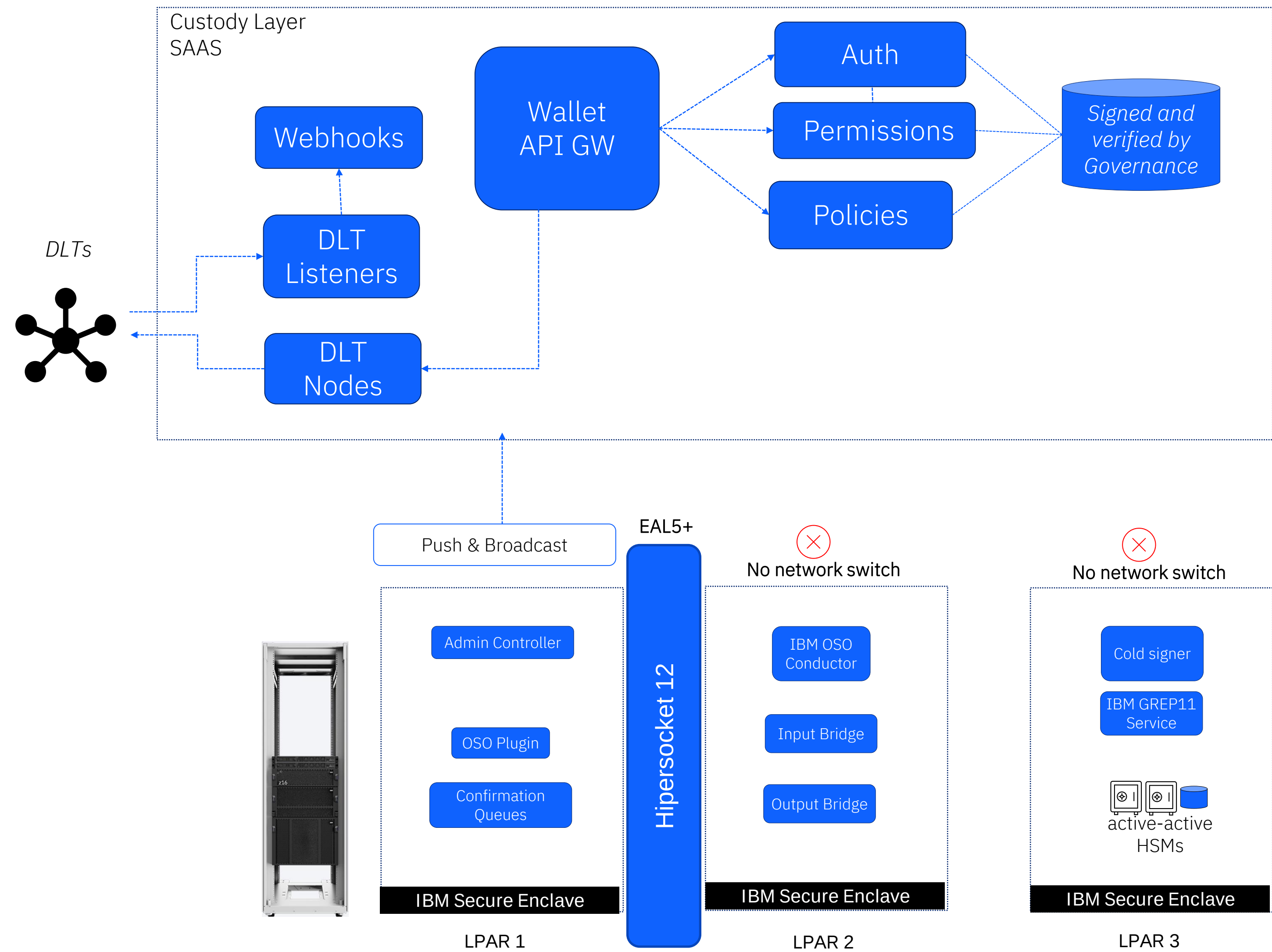
Cold Storage Signing Flow



7



Cold Storage Signing Flow



End

Trademarks

© 2025 International Business Machines Corporation

IBM, the IBM logo, IBM Z are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on <https://www.ibm.com/legal/copyright-trademark>.

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

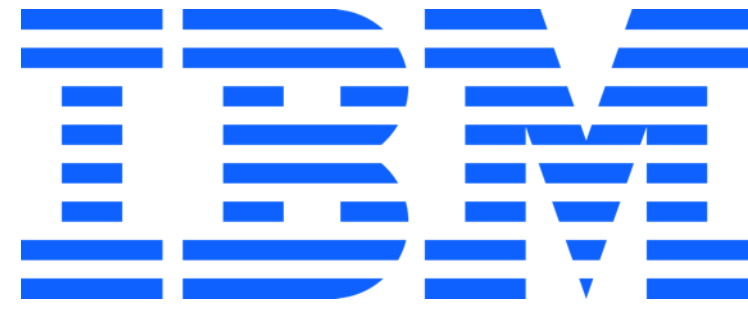
Client examples are presented as illustrations of how those clients have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

Not all offerings are available in every country in which IBM operates.

Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.

All names and references for organizations and other business institutions used in this deliverable’s scenarios are fictional. Any match with real organizations or institutions is coincidental.

All names and associated information for people in this deliverable’s scenarios are fictional. Any match with a real person is coincidental. Videos may show information about or belonging to third parties. Such videos do not suggest endorsement of third parties or their products or services.



Visit: <https://www.ibm.com/products/digital-asset-haven>

Additional Slides

Use the slides as needed to support specific topics

Multi-Party Computation (MPC)

Custom MPC Backup Deployments



Private Key Recovery

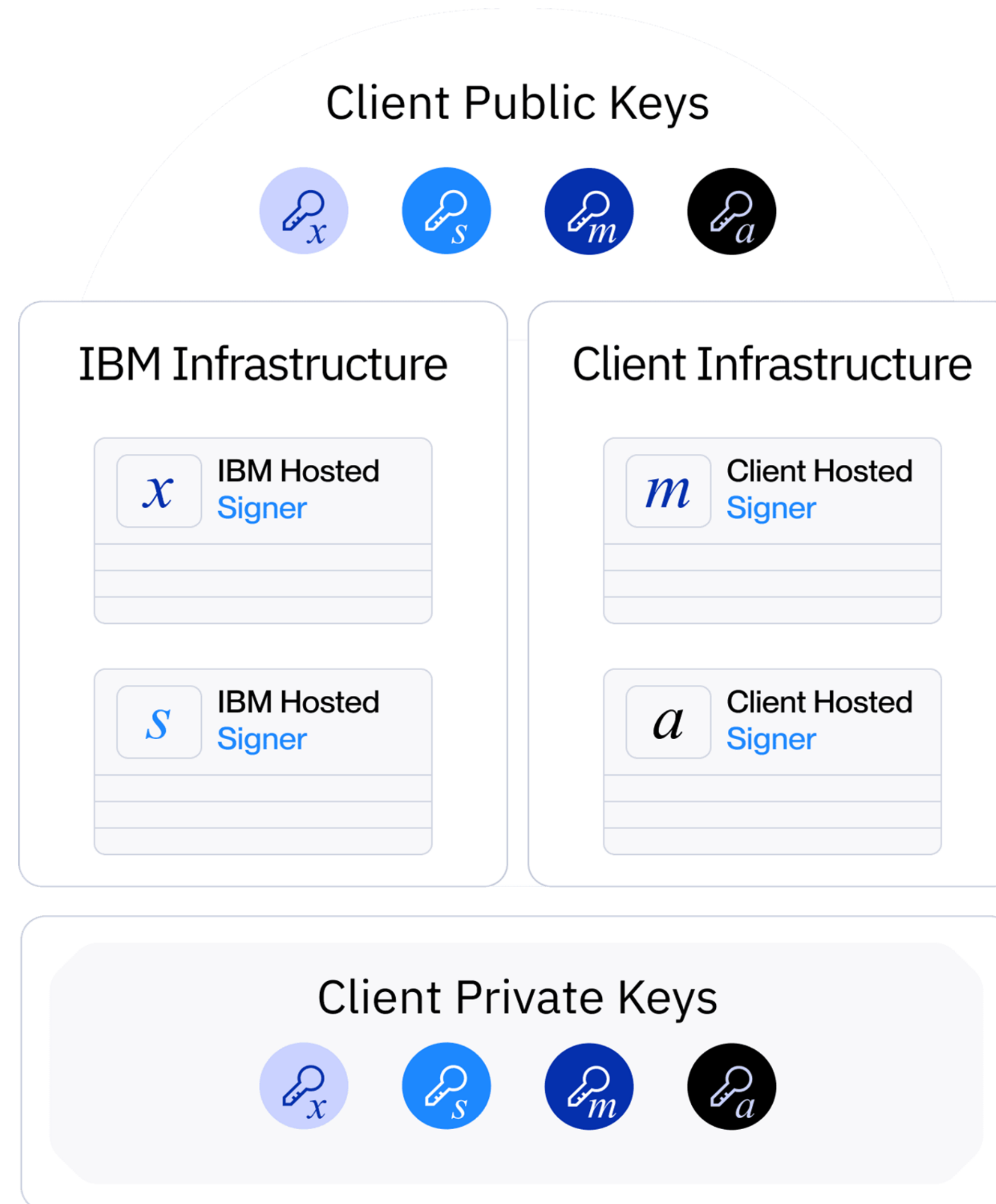
IBM's DRP focuses on safeguarding client keys, preventing misuse and unauthorized access, and ensuring their functionality. It consists of five tiers inspired by IANA, designed to protect client assets per different critical scenarios.



Passkey Recovery

IBM offers two passkey recovery options: additional credentials or passcodes, meeting high-security standards with 2FA. Users can add extra verification steps, and enterprise-level clients can request custom passkey recovery.

Local Backup Deployments - Configuration (1/3)



1. Customers generate asymmetric key pairs during cluster setup, sharing the public key(s) with Dfns.
2. Signers can be configured with individual or shared public keys.
3. The private key(s) remain securely in the customer infrastructure and can be stored in a cold storage environment.

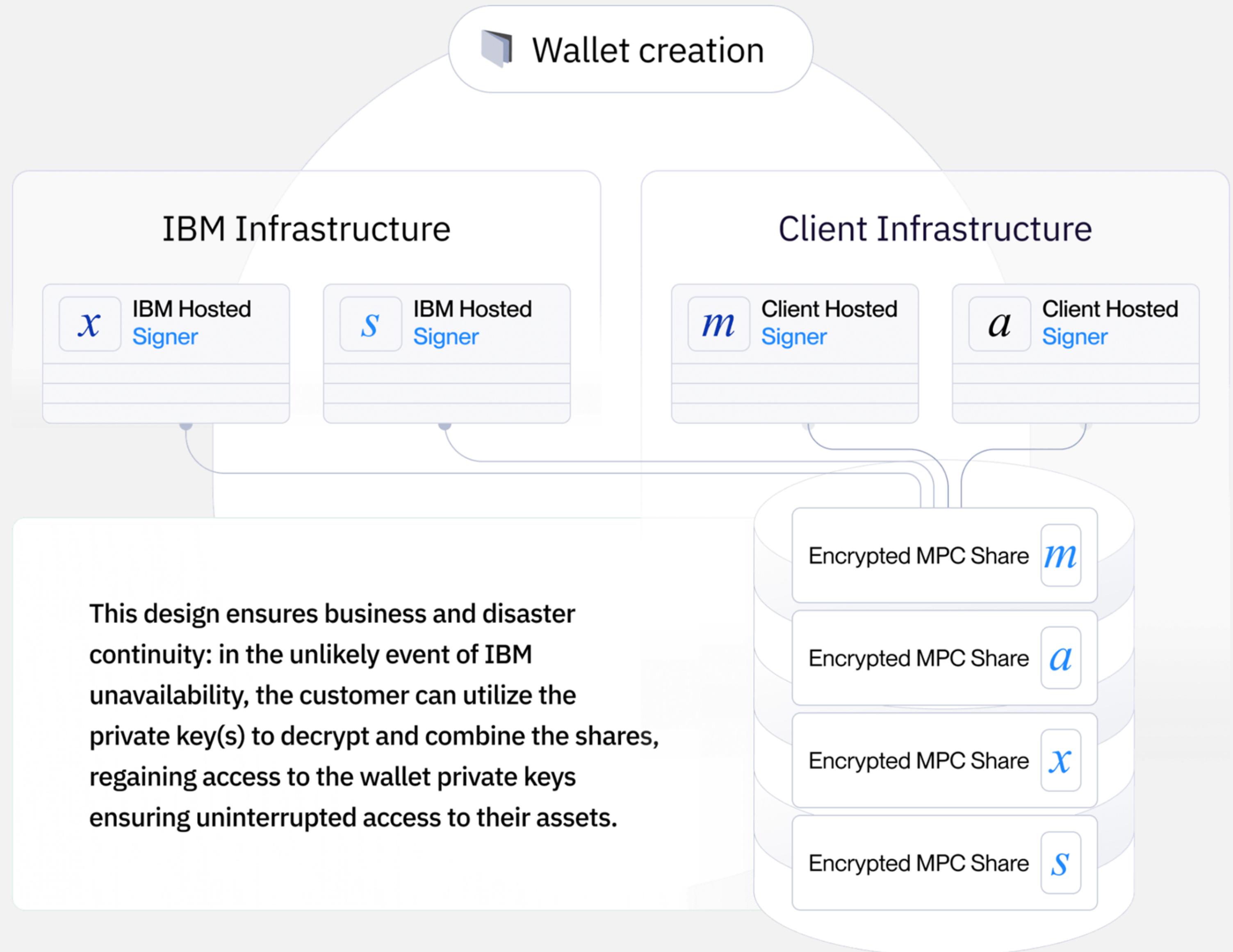
Local Backup Deployments - Configuration (2/3)



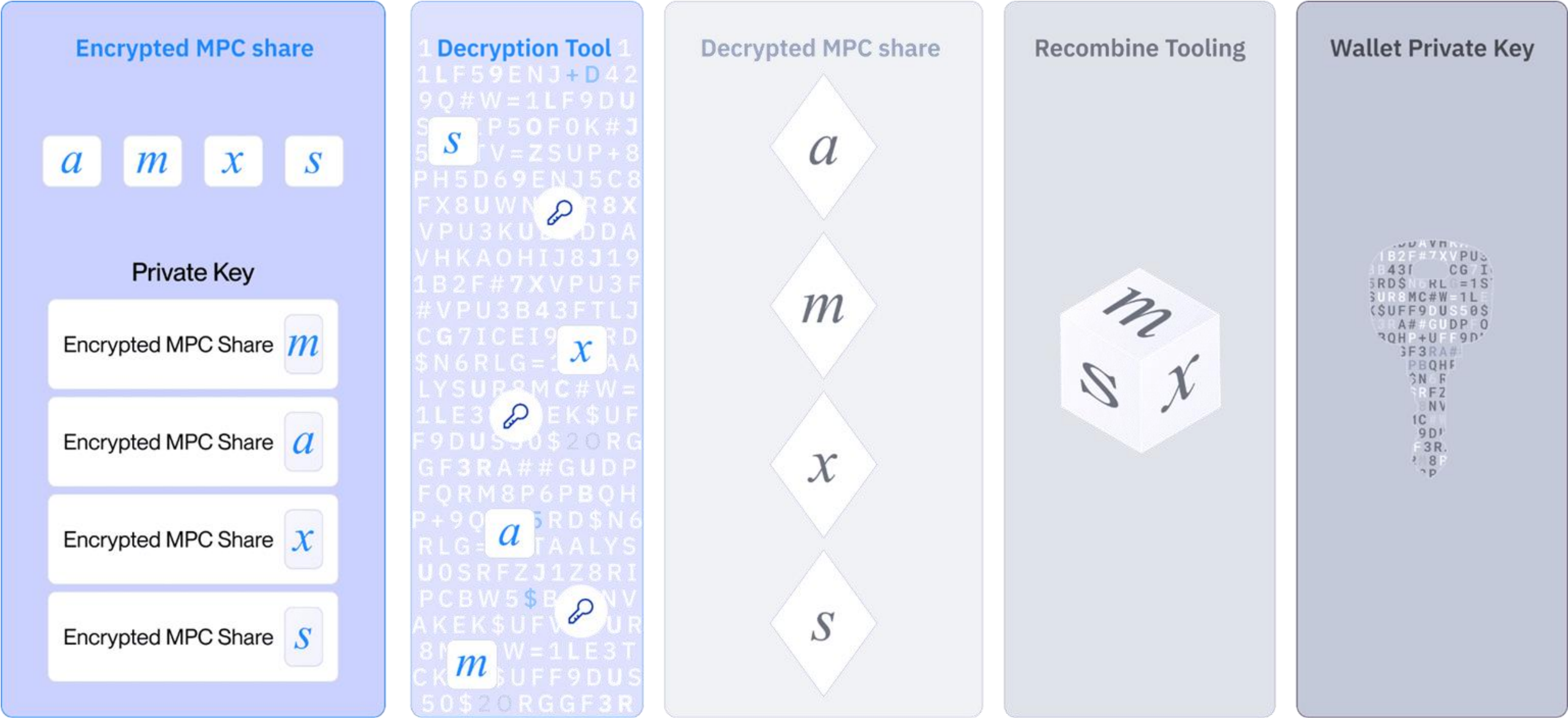
Signers encrypt the key shares using their associated public key.



Signers securely store the encrypted key shares in a synchronized S3 bucket, mirroring data between Dfns and the customer's infrastructure

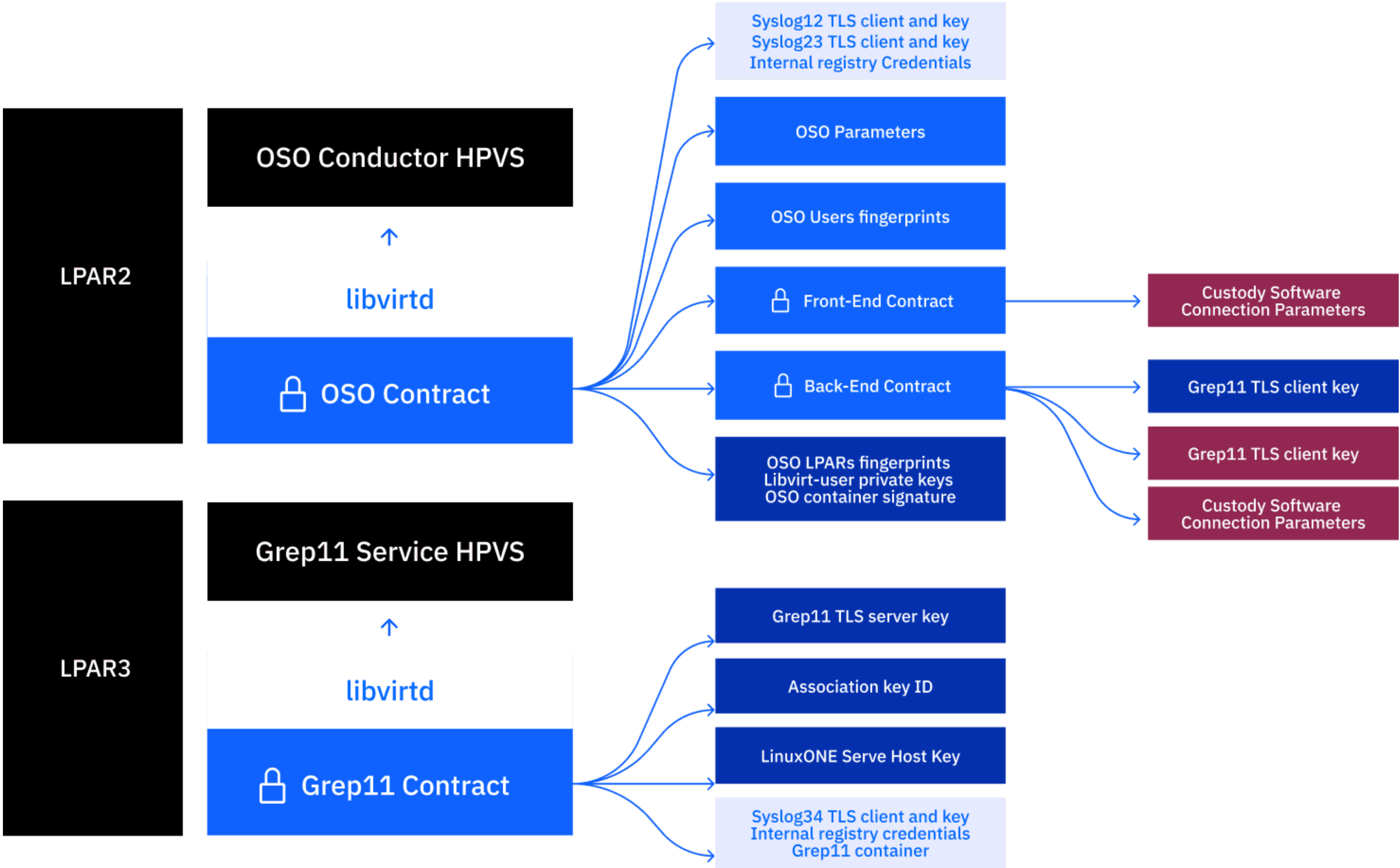


Local Backup Deployments - Configuration (3/3)



Offline Signing Orchestrator

Protecting Offline Signing Orchestrator (OSO)



Libvirtd service uses HPVS contracts to start up the secure enclave.

HPVS contracts are ciphered and protect all sensitive data.

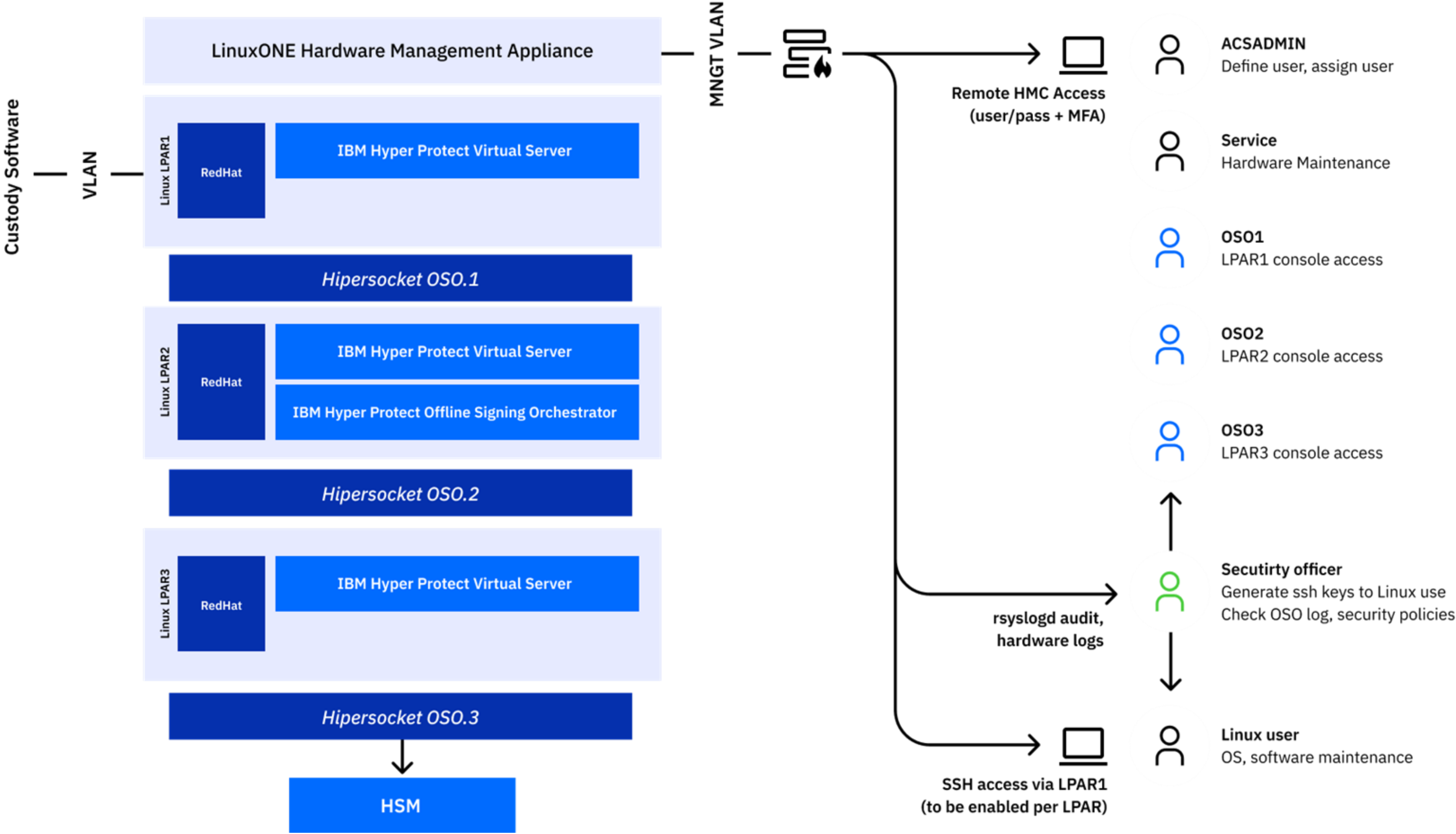
Linux administrators cannot get access to these values.

Linux administrators cannot tamper to these values.

IBM cannot uncypher these contracts.

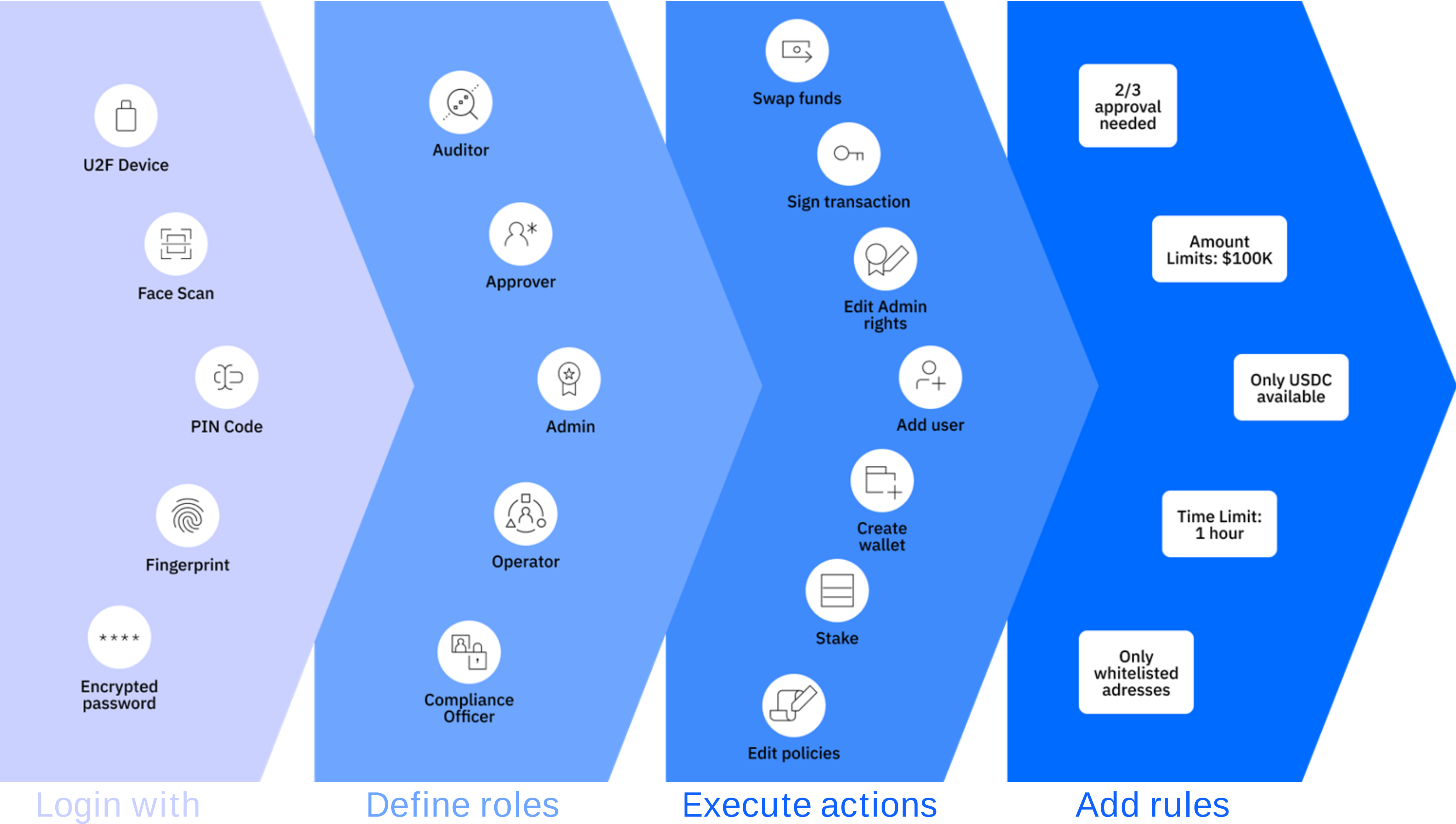
- Custody software (IBM Digital Asset Haven) sensitive data
- Connection sensitive data - Provided by a certificate authority
- OSO sensitive data - Includes OSO validators and admins user private key
- OSO Infrastructure sensitive data - Includes container signature

Ensuring integrity with Offline Signing Orchestrator (OSO)



Governance

Programmatic flow: Application-level objects & actions



Core Banking Integration

Indicative Core Banking Integration (“buy BTC”)

